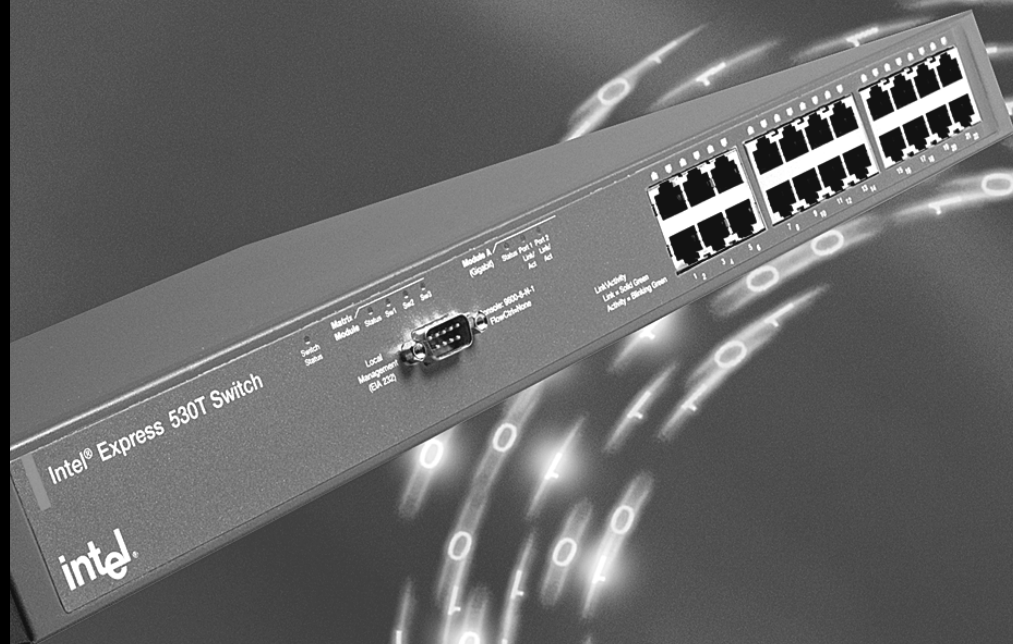


Intel® Express 530T Switch

User Guide



intel®

Year 2000 Capable

An Intel® product, when used in accordance with its associated documentation, is "Year 2000 Capable" when, upon installation, it accurately stores, displays, processes, provides, and/or receives date data from, into, and between 1999 and 2000, and the twentieth and twenty-first centuries, including leap year calculations, provided that all other technology used in combination with said product properly exchanges date data with it. Intel makes no representation about individual components within the product should they be used independently from the product as a whole.

Copyright © 2000, Intel Corporation. All rights reserved.
Intel Corporation, 5200 NE Elam Young Parkway, Hillsboro OR 97124-6497

Intel Corporation assumes no responsibility for errors or omissions in this manual. Nor does Intel make any commitment to update the information contained herein.

* Other product and corporate names may be trademarks of other companies and are used only for explanation and to the owners' benefit, without intent to infringe.

Contents

1.0 Setting up the Intel® Express 530T Switch	1
Management	1
Switch Features	2
Status LED	3
Port LEDs	3
Modules	4
Installing a Module	5
Module LEDs	6
Configuring Modules	6
Media Requirements	7
Straight-through vs. Crossover Cable	8
Stacking	9
2.0 Using the Intel® Express 530T Switch	11
What is a Switch?	12
Sample Configurations	13
Flow Control	14
Spanning Tree Protocol	14
Tagged Frames	15
Priority	15
Link Aggregation	16
Virtual LANs	17
GARP VLAN Registration Protocol (GVRP)	20
Internet Group Multicast Protocol	20
3.0 Using Intel® Device View 2.1	21
Installing Intel Device View	22
Starting Intel Device View	23
Installing a New Device	24
Using the Device Tree	25
Managing a Switch	27
Viewing RMON Information	28

4.0 Using the Web Device Manager 29

Accessing the Web Device Manager	30
Navigating the Web Device Manager	31
Using Management Screens	32
Configuring the Switch's IP Settings	33
Configuring a Port	34
Managing User Accounts	35
Configuring VLANs	37
Link Aggregation	42
Static MAC Addresses	43
Configuring Community Strings and Trap Receivers	44
Monitoring Switch Activity	45
Viewing/Changing Switch Information	46
Updating Switch Firmware	47
Saving Configuration Changes and Logging Out	49

5.0 Using Local Management 51

Accessing Management	51
Logon Screen	52
Navigation	53
Main Menu (Top Screen)	54
Configure Stack	55
IP Settings	56
Port Settings	57
Configure Optional Module	58
Stack Settings	59
View Stack Information	60
Configure Advanced Switch Settings	61
Configure Spanning Tree Protocol	62
Configure Spanning Tree for Ports	64
Forwarding and Filtering	65
Configure IGMP Snooping	66
Configure Static MAC Addresses	67
Configure Port Security	68

Configure MAC Address Filter Table	69
Configure Ethernet Multicast Filtering	70
Ethernet Multicast Filtering (Ports)	71
Port Mirroring	72
Link Aggregation	73
Broadcast Storm Control	74
Configure Management	75
Community Strings and Trap Receivers	76
User Accounts	77
How to Manage User Accounts	78
Update Firmware and Configuration Files	80
Reset and Console Options	81
Configure VLAN Operation Mode	82
Configure Port-based VLANs	83
Add a Port-based VLAN	84
Edit/Delete a Port-based VLAN	85
Edit VLAN Membership (Port-based)	86
Configure IEEE 802.1Q VLAN	87
Add an IEEE 802.1Q VLAN (Configure Port Membership)	88
Add an IEEE 802.1Q VLAN (Configure Port Tagging)	89
How to Configure 802.1Q VLAN	90
Edit/Delete an IEEE 802.1Q VLAN.....	92
Edit an IEEE 802.1Q VLAN (Configure Port Membership)	93
Edit an IEEE 802.1Q VLAN (Configure Port Tagging)	94
Configure VLAN ID for Untagged Traffic	95
GVRP and Ingress Filtering Settings	96
Monitoring (Network Statistics)	97
Switch Stack Overview	98
Port Traffic Statistics	99
Port Error Statistics	101
Packet Analysis	103
IGMP Snooping Status	104
Browse Address Table	105
VLAN and GVRP Status	107
Tools	108

Switch Event Log 109

Ping a Device 110

Upload Configuration Image File 111

Appendix: Technical Info **113**

About Configuration Files 113

Sample Configuration File 114

BOOT Menu 116

List of Factory Defaults 117

Troubleshooting/FAQs 118

Locating MIB files 120

Regulatory Information 121

Warnings 121

Limited Hardware Warranty 124

Limited Hardware Warranty (Europe only) 125

 Limitaiton de garantie du materiel (Europe) 126

 Garanzia limitata sull’hardware (valida solo in Europa).... 127

 Beschränkte Hardwaregarantie (Nur für Europa)..... 128

 Garantia limitada de hardware (solo para Europa) 129

Index **131**

Intel Customer Support **Last Page**

1

Setting up the Intel[®] Express 530T Switch

Overview

This guide provides information on configuring and managing the Intel[®] Express 530T Switch and is organized into these chapters:

- Chapter 1 - Information on the switch hardware and optional modules
- Chapter 2 - Information on using the switch in a LAN and advanced features such as link aggregation and Virtual LANs (VLANs)
- Chapter 3 - How to use Intel Device View
- Chapter 4 - How to use Web Device Manager
- Chapter 5 - Overview of Local Management

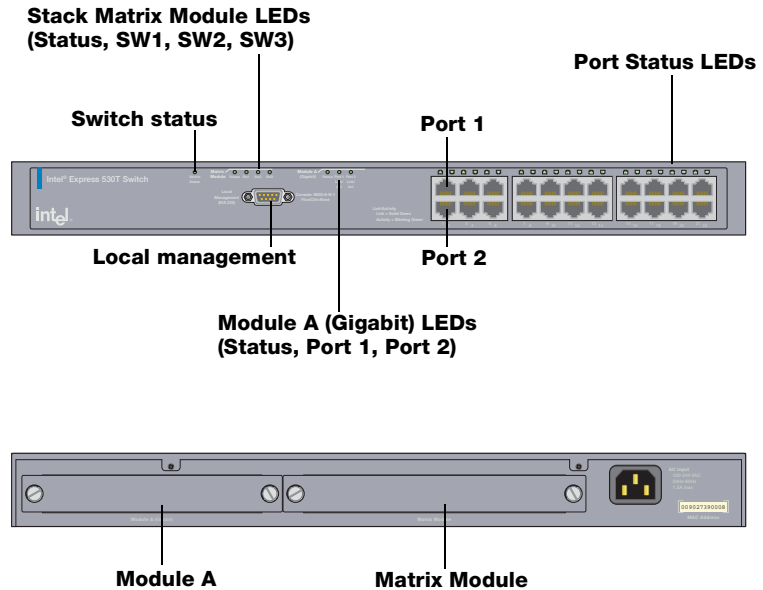
Management

Through the switch's built-in management you can configure the device and monitor network health. There are several methods for managing this switch; you can use one method or any combination.

- **SNMP management applications** such as Intel[®] Device View, LANDesk[®] Network Manager, or HP OpenView* are tailored for Intel products and show a graphical representation of the device (with the use of the proper MIB).
- **Onboard management** allows control over the device without using an SNMP application. The Web Device Manager provides a graphical interface; Local Management is a menu-driven interface.
- **Other SNMP-compliant applications** can manage 530T switches if you compile the switch's MIB files into that application.

Switch Features

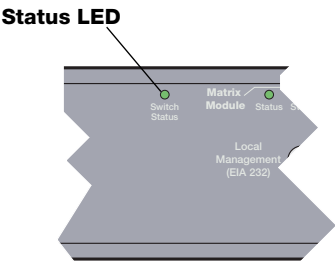
These are the major features of the 530T switch.



-
- Auto-negotiates speed, duplex, and flow control—10Mbps or 100Mbps *per port*.
 - Half- and full-duplex flow control.
 - Two-port expansion slot for the optional 1000Base-SX, 1000Base-LX, or 100/1000Base-T module.
 - Can be stacked with up to three 535T (member) switches.
 - Port settings can be configured manually through management.
 - Access menu-driven Local Management through the serial port or a Telnet session.
 - Access the graphic, Web-based, Web Device Manager through a Web browser.
-

Status LED

The Status LED is located to the left of the Matrix Module LEDs.



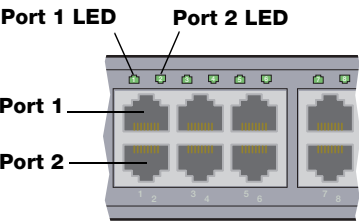
NOTE

When the switch is first powered on the Status LED is red for a couple of seconds before the diagnostic mode starts, then it turns orange.

LED	Status	Meaning
Status	Orange	Switch is performing diagnostics.
	Green	Diagnostics have passed, the switch is ready.
	Red	Diagnostics have failed.

Port LEDs

The LEDs above each port indicate port status and port activity.



LED	Status	Meaning
Left (Upper port)	Solid green	Device linked.
	Blinking green	Receiving traffic on that port.
	Off	No link detected.
Right (Bottom port)	Solid green	Device linked.
	Blinking green	Receiving traffic on that port.
	Off	No link detected.

About the 530T Switch

General

- The 530T switch is capable of auto-negotiating port speed and can operate at 10Mbps or 100Mbps per port. The switch matches the highest possible speed of an attached device.
- The 530T switch is capable of auto-negotiating port duplex and can operate at half- or full-duplex.

Cabling

- Use Category 5 or greater unshielded twisted-pair (CAT 5 UTP) cable when connecting 100Mbps devices to the switch.
- Use Category 3, 4, or 5 unshielded twisted-pair (CAT 3, 4, or 5 UTP) cable when connecting 10Mbps devices to the switch.
- Limit the cable length between devices to 100 meters (328 feet).
- Use a straight-through cable to connect the switch to a server or workstation. For more information on cabling, see pages 7 and 8.

Modules

The 530T switch accepts a Stack Matrix Module to connect with up to three member switches and an uplink module (Module A) to provide an additional two Gigabit ports.

The four modules supported by the 530T are:

- Stack Matrix Module (Connects to a maximum of three 535T [member] switches.) (ES530MSM)
- 1000Base-SX (ES530MSX)
- 1000Base-LX (ES530MLX)
- 100/1000Base-T (ES530MT)

NOTE

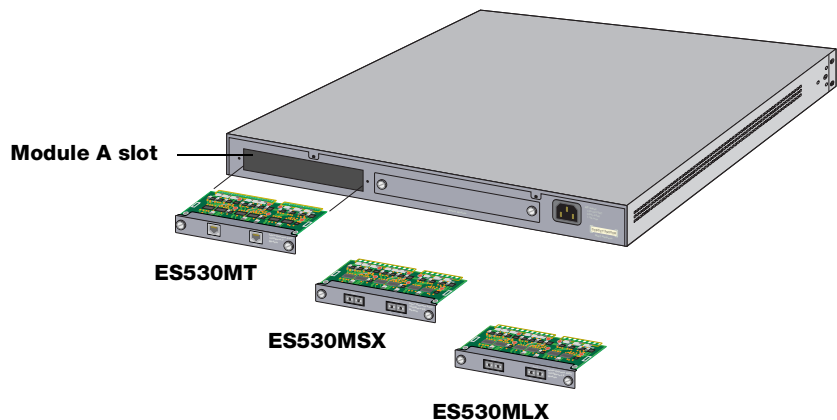
Install the Stack Matrix Module in the slot labeled Matrix Module.

Installing a Module

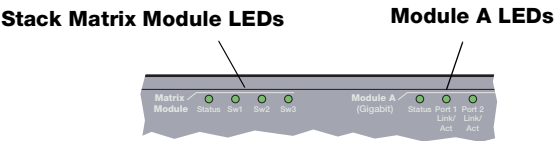
You can install only gigabit modules in the Module A slot located at the back of the 530T switch. Use the LEDs on the front of the switch to check the module's status.

Install the module in the switch

- 1 Unplug the power cord from the switch. Remove the panel from the expansion slot labeled Module A.
- 2 Align the module with the card guides inside the switch and slide the module into the slot. Press firmly to connect the module and secure it with the retaining screws.
- 3 Plug in the power cord.



Module LEDs



Stack Matrix Module LEDs

LED	Status	Meaning
Status	Off	No module present.
	Solid green	Module present.
SW1, SW2, SW3	Off	No link detected.
	Solid green	Switch connected to stack.

Module A (Gigabit) LEDs

LED	Status	Meaning
Status	Off	No module present.
	Solid green	Module present.
Ports 1, 2	Off	No link detected.
	Solid green	Device linked.
	Blinking green	Link with traffic.

NOTE
The 1000SX and 1000LX modules connect at only 1000Mbps and full-duplex.

Configuring Modules

Normally you do not need to make any changes to the optional modules because they are designed to configure themselves automatically for the attached device. However, you might need to configure the modules in order to communicate with older devices. You can use the Local Management or Web Device Manager to configure the 1000SX, 1000LX, or 1000T modules.

Media Requirements

Incorrect cabling is often the cause of network performance problems. Read the next two pages to make sure your cabling is correct.

NOTE

- 100 meters = 328 feet
- 200 meters = 656 feet
- 500 meters = 1640 feet
- 2 km = 2000 meters = 6560 feet
- 5 km = 5000 meters = 16400 feet

10Base-T

The 10Base-T Ethernet specification allows you to use CAT 3, CAT 4, or CAT 5 UTP cabling. The limit is 100 meters between any two devices.

100Base-TX

The 100Base-TX Fast Ethernet specification requires that you use CAT 5 UTP cabling to operate at 100Mbps. If you use lower grade cabling (CAT 3 or CAT 4) you may get a connection, but also experience data loss or slow performance. You're limited to 100 meters between any two devices.

1000Base-T

The 1000Base-T Gigabit specification requires that you use CAT 5 UTP cabling to operate at 1000Mbps. If you use a lower grade cabling you will experience either no connection or extreme data loss. The maximum distance between any two devices is 100 meters.

1000Base-SX/1000Base-LX

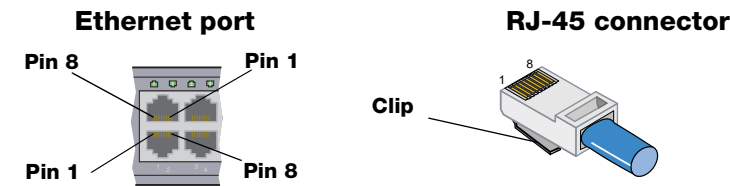
The optional 1000Base-SX and -LX Gigabit Modules provide a high-speed connection to another device up to 5 km away. The maximum distance depends on the type of cable used. Refer to the following table for a list of cable types and maximum distances. Use cables with an SC-type fiber optic connector.

Selecting the right cable

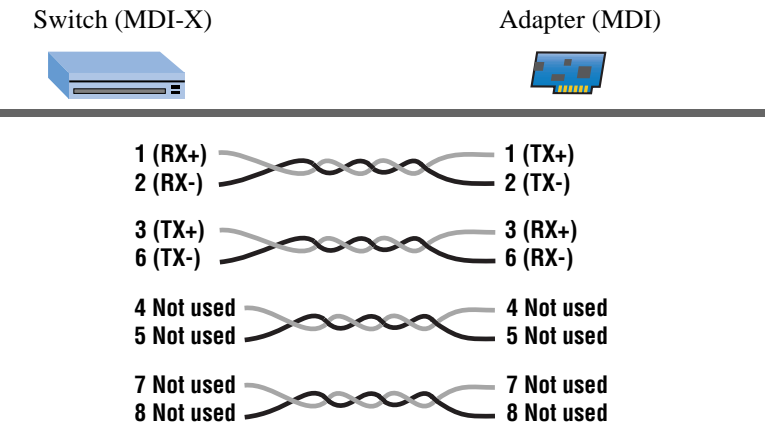
Media Type	Cabling Used	Maximum Distance
1000/100Base-T (Gigabit) Module	Category 5 (CAT 5) unshielded twisted pair cable	100m
1000Base-SX (Gigabit) Module	50/125 μm multimode	550m
	62.4/125 μm multimode	260m
1000Base-LX (Gigabit) Module	50/125 μm multimode	550m
	62.4/125 μm multimode	550m
	9/125 μm singlemode	5,000m

Straight-through vs. Crossover Cable

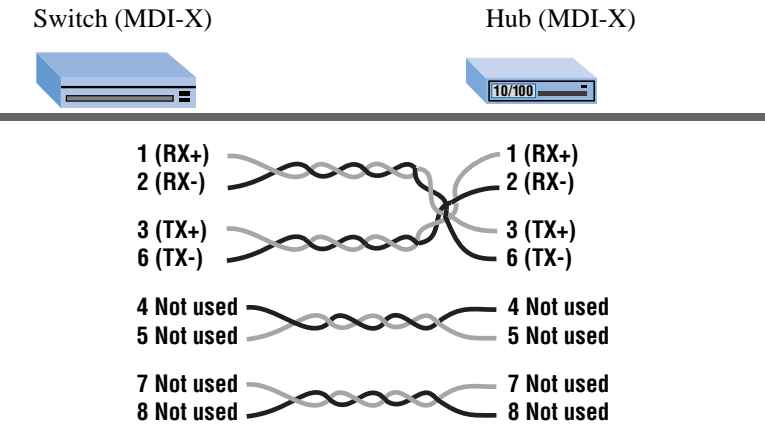
Switch ports are wired MDI-X, so use a straight-through cable to connect to a workstation or server (network adapter cards are wired MDI). To connect to another MDI-X port, use a crossover cable. Here are the pin arrangements for the switch's Ethernet port and the typical RJ-45 connector.



Straight-through UTP cable (for 100Base-TX)



Crossover UTP cable (for 100Base-TX)



NOTE
Pairs 4/5 and 7/8 are RX/TX when operating at 1000Mbps.

Stacking

The 530T switch can be stacked with up to three 535T switches. Stacking allows for a single point of management for all switches.



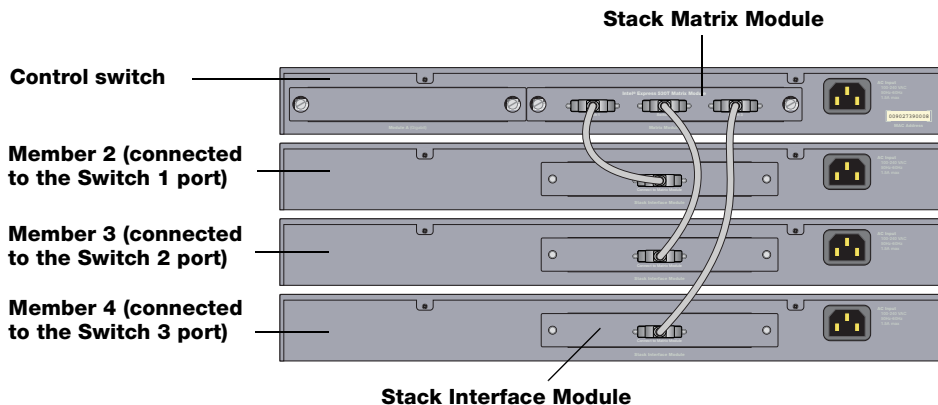
About a stack

- There can be only one 530T switch in a stack.
- The 530T switch requires the installation of a Stack Matrix Module to stack it with a 535T. (Only one Stack Matrix Module is needed for the entire stack.)
- The 530T can be stacked only with 535T switches.
- You can stack up to three 535T switches with a 530T.
- In a stack, the 530T is the control switch and the 535Ts are the member switches.
- The member switches are all managed through the control switch's management interface.
- There is only one IP address for the entire stack of switches (the control switch's IP address).
- There can be only one instance of Spanning Tree, regardless of the number of switches in the stack.
- Ports from any switch can be members of any VLAN.
- For link aggregation, the anchor ports are 1, 7, 15 for both the control and member switches. You can also link aggregate the module ports on the control switch (530T).
- You can only link aggregate ports on the same switch.

Assemble a stack

To stack a 530T with 535Ts, you need to purchase a Stack Matrix Module.

- 1 Insert the Stack Matrix Module into the slot in the back of the 530T, labeled Matrix Module, and tighten the screws.



- 2 Run a cable from the slot in the back of the 535T, labeled Stack Interface Module, to the control switch's Stack Matrix Module, where it reads "Switch 1." This connection makes this 535T switch Member 2 in the stack.
- 3 Repeat step 2 until you have added all member switches (535Ts) to the stack. You can add a total of three member switches.
- 4 Power on the control switch.

NOTE

When setting up a stack, stack the 535T switches in the order in which they are connected to the Matrix Module.

The 535T connected to the Switch 1 port of the Matrix Module would be the switch directly under the control switch, the 535T connected to the Switch 2 port would be underneath that, etc.

This makes it easier to determine which switch is which when managing them.

Which switch is which in a stack

In a stack of switches, the 530T is the control switch and the 535Ts are member switches.

The switch that you connect to the port labeled Switch 1 in the 530T's Stack Matrix Module is referred to in the Web Device Manager and Local Management as Member 2. The switch connected to the port labeled Switch 2, is Member 3. And the switch connected to the port labeled Switch 3, is Member 4.

2

Using the Intel® Express 530T Switch

Overview

This section provides an overview for using the Intel® Express 530T Switch within a network. The chapter covers the basic differences between a switch and hub, basic switching features, such as flow control and Spanning Tree, and a discussion of the more advanced features such as link aggregation and the types of VLANs available on the switch.

If you are already familiar with switching technology you can skip ahead to a particular section within the chapter. Following is a basic overview of the chapter and the pages where you can find a particular topic.

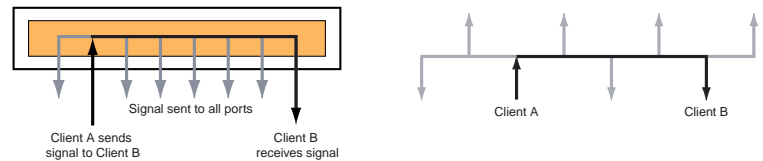
- **Sample Configurations** page 13
- **Flow Control** page 14
- **Spanning Tree Protocol** page 14
- **Tagged Frames** page 15
- **Priority** page 15
- **Link Aggregation** page 16
- **VLANs** page 17
- **GVRP** page 20
- **Internet Group Multicast Protocol** page 20

What is a Switch?

A switch segments traffic, providing each port its own collision domain. This is different than a hub where all ports belong to the same collision domain.

Segments and hubs

Hubs combine multiple wires so all attached devices behave as though they are on the same wire. Since the devices share the same segment, data sent by one device is retransmitted to all devices on the same hub. This is equivalent to having all devices connected in a bus topology as illustrated below.

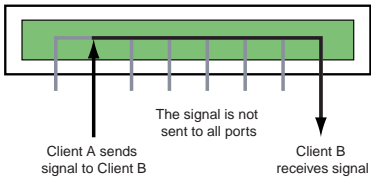


The disadvantage is all devices must share the total available bandwidth. The more devices that are attached to the hub results in less bandwidth for each user. Also, network performance suffers since all devices receive traffic and collisions from other users because the hub retransmits data across all ports.

Switches

Switches send traffic only to specific ports, rather than transmit data across all ports. This means that each device attached to the switch receives fewer collisions and the entire bandwidth is available to the device.

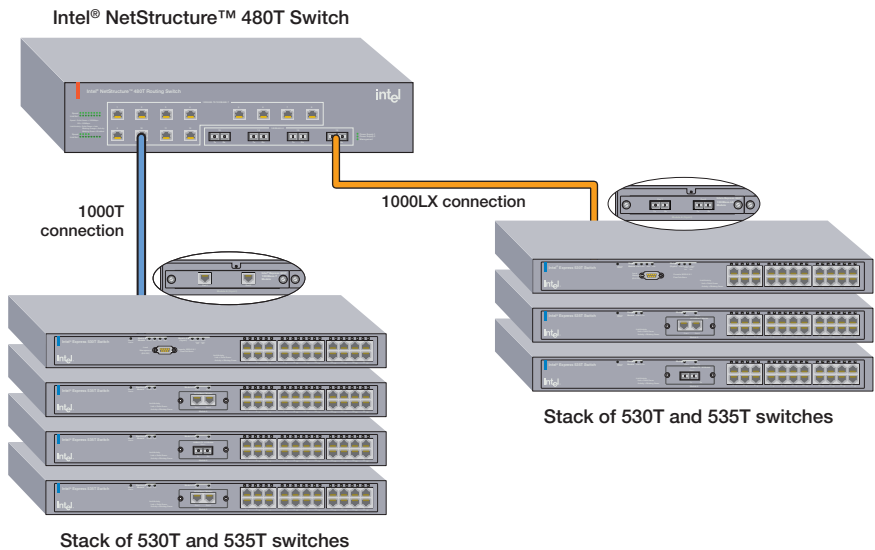
MAC Address	Port
006011FB34DB	2
00A027D36FAA	8



The switch maintains a table that associates a device’s MAC address to a port on the switch. When Client A communicates with Client B, the switch looks in the table to determine which port Client B is attached to and then forwards the traffic to that port. If a device sends traffic to an address that is not in the table (or sends broadcast or multicast traffic) the switch sends the traffic out to all ports on the switch. When the switch receives a response it updates the table with the new address.

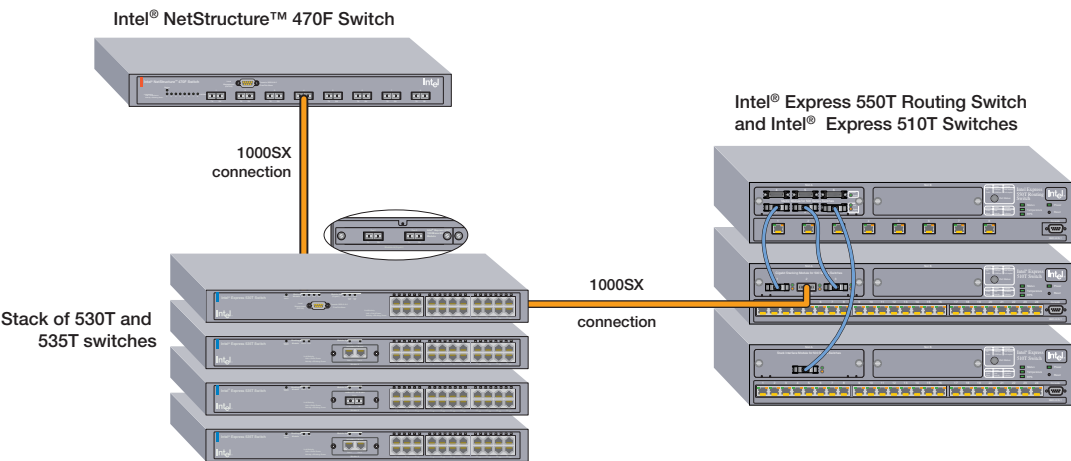
Sample Configurations

The following examples illustrate how the 530T switch can be used in a network.



Using the 530T

The example below shows how a stack of 530/535 switches connects with a stack of 550/510 switches (they cannot be in the same stack). This example also demonstrates the 530T's gigabit uplink by connecting it to a 470F switch.



Flow Control

During times of heavy network activity, the switch's port buffers can receive too much traffic and fill up faster than the switch can send the information. In cases like this, the switch tells the transmitting device to wait so the information in the buffer can be sent. This traffic control mechanism is called flow control.

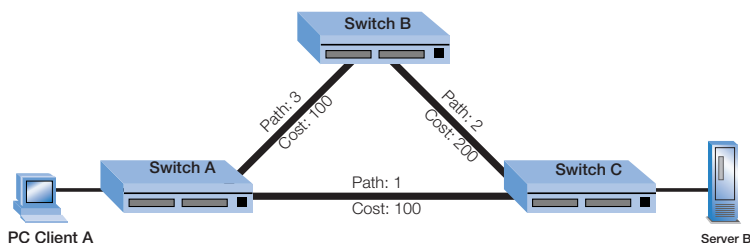
The method of flow control depends on whether the port is set to full- or half-duplex. If a port is operating at half-duplex, the switch sends a collision (also called backpressure) which causes the transmitting device to wait. If the port operates at full-duplex, the switch sends out an IEEE 802.3x PAUSE frame. You can enable or disable flow control for each port on the Express 530T switch.

Spanning Tree Protocol

Spanning Tree helps to prevent any loops within the network topology. A loop can occur if there is more than one path for information to travel between devices. The Spanning Tree Protocol works by determining the "cost" of a connection. For example, if two devices are connected by two links, Spanning Tree uses the connection with the lowest cost and blocks the second connection from working.

Spanning Tree prevents loops by allowing only one active path between any two network devices at a time. However, you can also use this behavior to establish redundant links between devices which can take over in the event the primary link fails.

The 530T supports one instance of Spanning Tree per switch (or per stack of switches).



In this example, Client A can communicate with Server B over two different paths. The primary path is Path 1 because the cost of the connection between switches A and C is lower than the cost between switches A, B and C. If the primary path fails, traffic is sent over the backup path automatically.

Tagged Frames

The 802.1D (1998 Edition) and 802.1Q specifications published by the IEEE (Institute of Electrical and Electronic Engineers) extends Ethernet functionality to add tag information to Ethernet frames and propagate these tagged frames between bridges (for example, a switch). The tag can carry priority information, VLAN information, or both and allows bridges to intelligently direct traffic across the network.

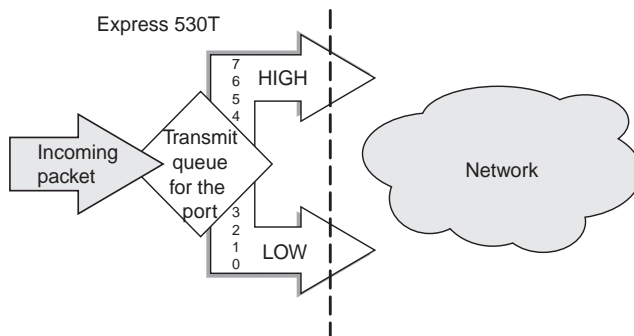
For outgoing (egress) packets you can specify whether you want the packets to be tagged or untagged. For incoming (ingress) packets you can set the ingress filtering so that packets are forwarded to a specific port as long as that port is a member of the VLAN. You can set a Port VLAN Identifier (PVID) so that if untagged traffic goes to that port, the packet inherits the VLAN Identifier (VID) of the port.

Priority

The IEEE 802.1D (1998 Edition) specification incorporates IEEE 802.1p and defines information in the frame tag to indicate a priority level. When these tagged packets are sent out on the network, the higher priority packets are transferred first. Priority packet tagging (also known as Traffic Class Expediting) is usually set on the LAN adapter in a PC and works with other elements of the network (switches, routers) to deliver priority packets first. The priority level can range from 0 (low) to 7 (high).

The 530T switch can read the priority tags and forward traffic on a per-port basis. The switch uses two priority queues per port and routes traffic to a queue depending on the packet's tag. For example, when a packet comes into the switch with a high priority tag, the switch routes the packet to its high-priority queue.

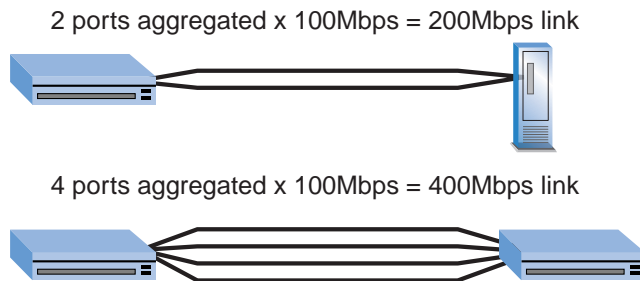
Even though there are eight priority levels, the 530T switch can route a packet into only one of the two queues. The switch maps levels 0-3 to the low queue (the default) and levels 4-7 to the high queue. If a packet is untagged, the switch determines the best way to send the packet.



Link Aggregation

Link aggregation allows you to combine from 2 to 8 (adjacent) ports so that they function as a single high-speed link. For example, link aggregation is useful when making connections between switches or to connect servers to the switch.

Link aggregation, sometimes known as port trunking, can be used to increase the bandwidth to some devices. Link aggregation can also provide a redundant link for fault tolerance. If one link in the aggregation fails, the switch balances the traffic among the remaining links.



To aggregate ports, you must link an “anchor” port with an adjacent port. The 530T switch supports up to four link aggregation groups (anchor ports 1, 7, 15). This includes one link aggregation group for the two module ports.

Guidelines

- The switch treats aggregated links as a single port. This includes Spanning Tree and VLANs.
- All ports share the same settings as the anchor port. You can change anchor port settings, but you cannot configure other ports in the link.
- When a port is configured as a member of an aggregated link, it immediately adopts the characteristics of the anchor port. When a port is no longer a member of an aggregated link, the characteristics are reset to the default settings (autonegotiate speed/duplex, flow control enabled).
- If a port is part of an aggregated link, it cannot be configured as the target port for a port mirror. However, a port in an aggregated link can serve as the source port for a port mirror.
- When a 530T is stacked with one or more 535T switches, you cannot aggregate ports that belong to separate switches. The 530T supports up to four link aggregation groups, and each 535T supports up to three.

Virtual LANs

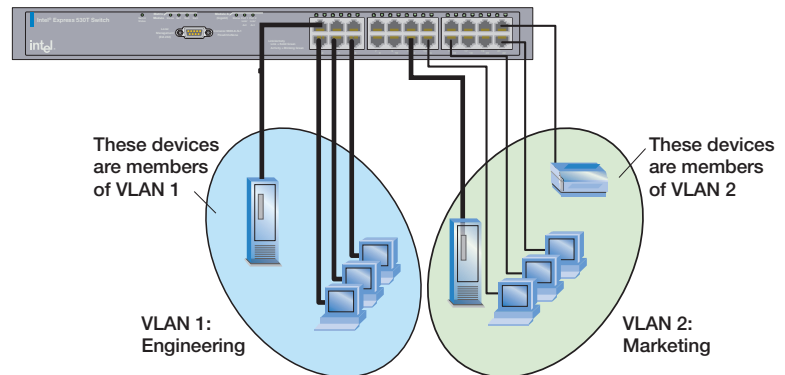
A Virtual LAN is a logical network grouping that allows you to isolate network traffic so members of the VLAN receive traffic only from other members. Creating a VLAN is the physical equivalent of moving a group of devices to a separate switch (creating a Layer 2 broadcast domain). The advantage of VLANs is that you can reduce broadcast traffic for the entire switch and increase security, without changing the wiring of your network.

The Express 530T switch supports two types of VLANs:

- Port-based
- IEEE 802.1Q (tag) -based

Port-based VLANs

This is the simplest and most common form of VLAN. In a port-based VLAN, the system administrator assigns the switch's ports to a specific VLAN. For example, the system administrator can designate ports 2, 4, 6, and 9 as part of the engineering VLAN and ports 17, 19, 21, and 22 as part of the marketing VLAN. The advantage of port-based VLANs is that they are easy to configure and all changes happen at the switch so they are transparent to the users. The 530T supports a maximum of 24 port-based VLANs. A port can belong to only one VLAN at a time.



If a user changes location, the system administrator reassigns the port to the new VLAN. Another advantage is if a hub is connected to a port that is part of a VLAN, all devices connected to the hub are also part of the VLAN. The disadvantage is that there is no way to exclude an individual device on that hub from becoming part of the VLAN.

When a 530T switch is stacked with one or more 535T switches, ports from any of the switches can be members of a port-based VLAN.

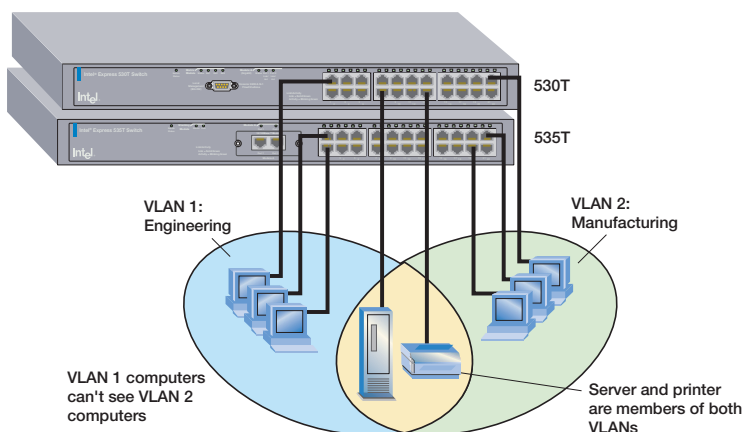
IEEE 802.1Q (tag)-based VLANs

The second type of VLAN supported by the 530T switch is based on the IEEE 802.1Q specification. The specification provides a uniform way for creating VLANs within a network and allows the creation of a VLAN that can also span across the network. Until recently, VLAN implementation was vendor specific so it was not possible to create a VLAN across devices from different vendors.

NOTE

When a 530T is stacked with one or more 535T switches, ports from any/all of the switches can be members of each VLAN.

The 802.1Q VLAN works by using a tag added to the Ethernet frames. The tag contains a VLAN Identifier (VID) that identifies the frame as belonging to a specific VLAN. These tags allow switches that support the 802.1Q specification to segregate traffic between devices and communicate a device's VLAN association across switches.



There are multiple advantages to implementing 802.1Q VLANs. First, it helps to contain broadcast and multicast traffic across the switch thus improving performance. Second, ports can belong to more than one VLAN. Third, VLANs can span multiple switches that support the 802.1Q specification. Finally, it can provide security and improve performance by logically isolating users and grouping them together. The 530T switch supports up to 2047 tag-based VLANs.

A logical grouping can be mapped to a work group. For example, you can create a VLAN that groups all the users from the engineering department into one VLAN. A benefit of this logical grouping is that it can improve performance by cutting down traffic that belongs to a different logical group (for example, marketing), improve security (engineering can't see marketing), and ease moves since the user doesn't have to be physically located in the same group to participate in the VLAN.

When a 530T switch is stacked with one or more 535T switches, ports from any/all of the switches can be members of a tag-based VLAN.

On the 530T switch, overlapping VLANs can be supported through the use of 802.1Q-capable devices. However, for non-802.1Q-capable devices, overlapping VLANs can be supported by implementing an asymmetric VLAN on the switch (see references below for more information). An asymmetric VLAN is a type of 802.1Q configuration where endstations send traffic on one VLAN and receive traffic on another VLAN. The 530T switch can support asymmetric VLANs.

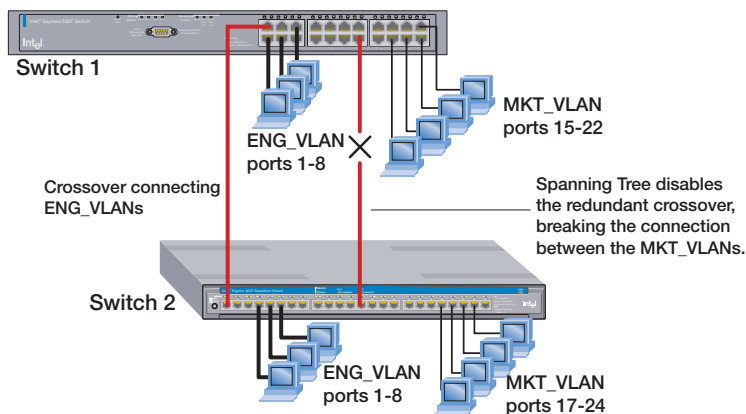
To learn more about asymmetric VLANs, see <http://support.intel.com/support> or refer to IEEE 802.1Q Specification Annex B.1.3.

Spanning Tree and VLANs

The 530T supports the Spanning Tree Protocol across the entire switch (or stack of switches), not per VLAN. If a loop occurs in a VLAN the port is disabled and all VLAN traffic over that port is blocked.

A good example of this can be seen below. Both Switch 1 and Switch 2 have two port-based VLANs configured. Crossover cables connect the ENG_VLAN on Switch 1 to ENG_VLAN on and Switch 2. Crossover cables also connect the MRKT_VLAN on Switch 1 to the MRKT_VLAN on Switch 2. When Spanning Tree is enabled, the redundant link between the MRKT_VLANs is blocked and those VLANs can no longer communicate.

When the switch is running 802.1Q VLANs, Spanning Tree is required for GARP VLAN Registration Protocol (GVRP) to work properly.



GARP VLAN Registration Protocol (GVRP)

Since IEEE 802.1Q VLANs can span networks, it poses a challenge for network administrators to manage changes to the VLAN. The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) provides a dynamic mechanism for switches to share topology information and manage changes with other switches. This alleviates the network administrator from manually propagating VLAN configuration information across switches.

GARP is defined by the IEEE 802.1D (1998 Edition) specification and is the mechanism used by switches and end nodes to propagate VLAN configurations across the network domain. GVRP uses GARP as a foundation to propagate VLAN configurations to other switches. Devices that support GVRP transmit their updates to a known multicast address that all GVRP-capable devices monitor for information updates.

Sending GVRP messages between switches accomplishes these tasks:

- Dynamically adds or removes a port from participating in a VLAN
- Sends updates about the switch's own VLAN configuration to neighboring GVRP-capable devices
- Integrates dynamic and static VLAN configurations within the same switch. Static VLAN configurations are created by the user on the switch for devices that don't support GVRP

Dynamically created VLANs are not saved in the switch's memory. When the device that is sending out the GVRP updates is disabled or rebooted the dynamic VLAN is removed.

NOTE

The 530T supports a maximum of 24 IGMP sessions, with a maximum of 32 multicast groups per session. These parameters are the same whether the 530T is standalone or in a stack.

Internet Group Multicast Protocol

Under normal circumstances, multicast traffic is broadcast by the switch to all ports. For multicast traffic based on the IGMP (Internet Group Multicast Protocol), the switch can optimize the broadcasting of multicast traffic by forwarding multicast traffic to only the ports that require it.

IGMP snooping is a feature that allows the switch to forward multicast traffic intelligently. The switch "snoops" the IGMP query and report messages and forwards traffic to only the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

IGMP requires a router that records the presence of multicast groups on its subnets and keeps track of group membership. It is important to remember that multicasting is not connection oriented, so data is delivered to the requesting hosts on a best-effort level of service.

3

Using Intel® Device View 2.1

Overview

Intel Device View allows you to manage the Intel® Express 530T Switch and other supported Intel networking devices on your network.

Intel Device View provides these features:

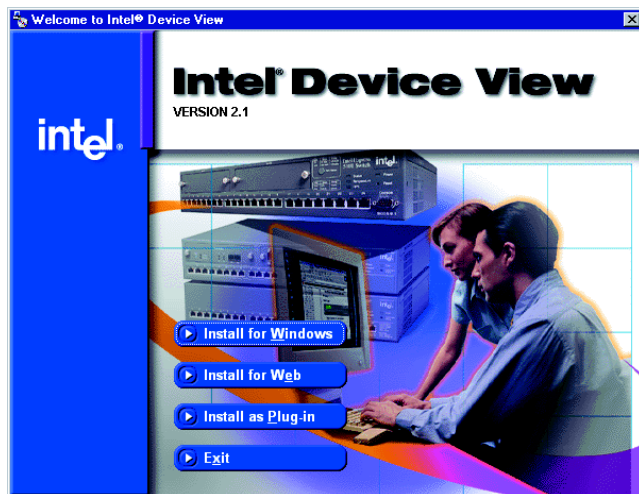
- The ability to configure new network devices
- Graphical device manager for Intel switches, hubs, and routers
- Autodiscovery, which finds supported Intel devices on the network
- The Device Tree, which shows all the supported devices detected on your network
- Remote Network Monitoring (RMON)
- Web or Windows* platform
- Plug-in to HP OpenView*, IBM Tivoli NetView*, and Intel LANDesk® Network Manager
- Other useful tools such as a TFTP server

Installing Intel Device View

Before you install Intel Device View, make sure your PC meets the system requirements in the *Intel Device View User Guide*, which is included on the Intel Device View CD-ROM.

To install Intel Device View

- 1 Insert the Intel Device View CD-ROM in your computer's CD-ROM drive. The Intel Device View installation screen appears. If it doesn't appear, run `autoplay.exe` from the CD-ROM.



- 2 Choose the version of Intel Device View you want to install.
 - Click **Install for Windows** to install Intel Device View for use on this PC only.
 - Click **Install for Web** to install Intel Device View on a Web server. You will be able to access the Device View server from any PC on your network with Internet Explorer* 4.0x or later.
 - Click **Install as Plug-in** to install Intel network device support for HP OpenView, IBM Tivoli NetView, or Intel LANdesk Network Manager. This option is not available if you don't have OpenView, Net View, or LANdesk Network Manager installed on the PC.
- 3 Follow the on-screen instructions in the installation program.

Starting Intel Device View

Install either the Windows or Web version of Intel Device View.

Windows version

From your desktop, click Start and then point to Programs > Intel Device View > Intel Device View - Windows. Intel Device View's main screen appears.

Web version

- From your desktop, click Start and then point to Programs > Intel Device View > Intel Device View - Web. Intel Device View's main screen appears.
- To view Intel Device View from another PC on your network, type the following URL. In the example shown below, the URL is entered into the Address field for Internet Explorer.

<http://servername/devview/main.htm>

where *servername* is the IP address or name of the server where Intel Device View is installed.

Intel Device View's main screen appears.

NOTE

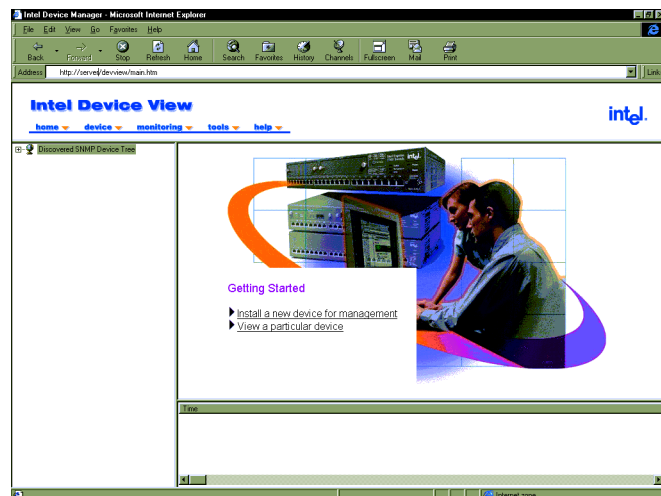
These are the requirements if you want to use the Web version of Device View:

Web browser

Internet Explorer 4.0 or newer

Web server

Internet Information Server (IIS) 2.0 or newer
Peer Web Services*
Netscape Enterprise* Web server 3.01 or later.



Installing a New Device

After you've installed a new switch on your network, you can use Intel Device View's Device Install Wizard to configure it for management.

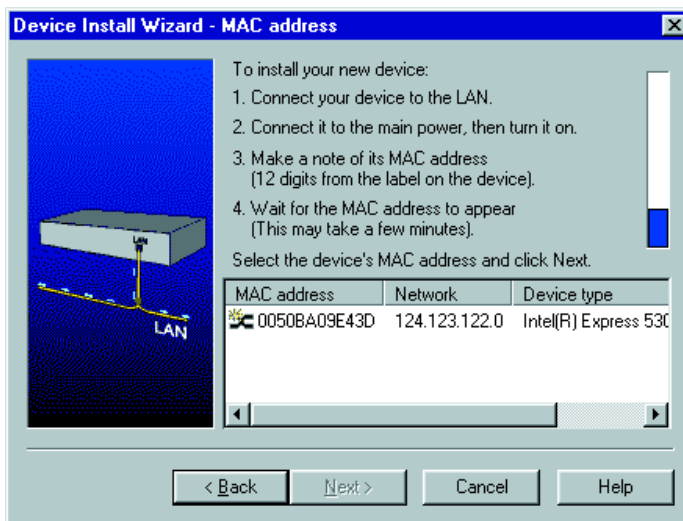
To install and configure a new switch for management

NOTE

The 530T sends BootP requests for several minutes; after that time, if no IP has been entered, the switch stops sending the request and continues to boot.

In a stack of switches, only one MAC address (the control switch's MAC address) is discovered.

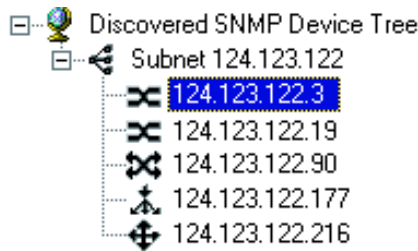
- 1 Start Intel Device View. The Device Install Wizard appears. If it doesn't appear, click Install from the Device menu or double-click the appropriate MAC address in the Device Tree under Unconfigured Devices. (The MAC address is located on the rear of the switch.)
- 2 On the Device Install Wizard - Start screen, click Next.
- 3 On the Device Install Wizard - MAC Address screen, click the MAC address of the new switch and then click Next.



- 4 Follow the instructions in the wizard to assign an IP address and a name to the switch (or stack of switches).









Using the Device Tree

When you start Intel Device View, the Device Discovery service begins searching for supported Intel network devices on your network. As it discovers devices, the Device Discovery service adds an icon for each device to the Device Tree on the left side of the screen.



Different states of the 530T switch are represented by unique icons in the Device Tree.

Device Tree icons

	Device Tree root
	Subnet
	Intel Express Switch (if non-responding the icon is red)
	Unconfigured Intel Express Switch
	Group of Intel Express Switches
	Intel Express Router
	Intel Express Switch (Layer 3 capable)
	Intel Express Stackable Hub

The Device Tree works much like Windows Explorer. To expand the root or a subnet, click the (+) next to the icon. To collapse the view, click the (-) next to the icon. Double-click a device icon to view the device image.

To add a device to the Device Tree

Use this procedure if the device does not automatically appear after installation.

- 1 Right-click anywhere on the Device Tree.
- 2 On the menu that appears click Add Device.
- 3 In the Add Device dialog box, type the IP address of the switch you want to add.
- 4 Fill in the other fields, as appropriate.
- 5 Click OK.

The new switch's icon appears in the Device Tree.

To refresh the Device Tree

- 1 Right-click anywhere on the Device Tree.
- 2 On the menu that appears click Refresh.

Refreshing the Device Tree updates it to show any newly discovered devices and changes in device status.

To delete a device from the Device Tree

- 1 Right-click the device you want to remove from the Device Tree.
- 2 On the menu that appears click Delete.

Deleting a device from the Device Tree does not affect the actual device.

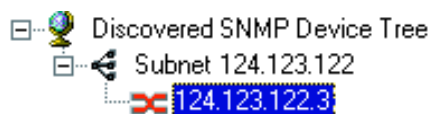
To find a device in the Device Tree

- 1 Right-click anywhere on the Device Tree.
- 2 On the menu that appears click Find.
- 3 In the Find Device dialog box, type the IP address of the device you want to find in the tree.
- 4 Click OK.

The device's icon is highlighted in the Device Tree.

Losing contact with a device

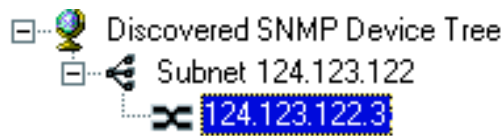
If Intel Device View loses contact with a switch, it replaces the switch icon with the non-responding switch icon, which is red.



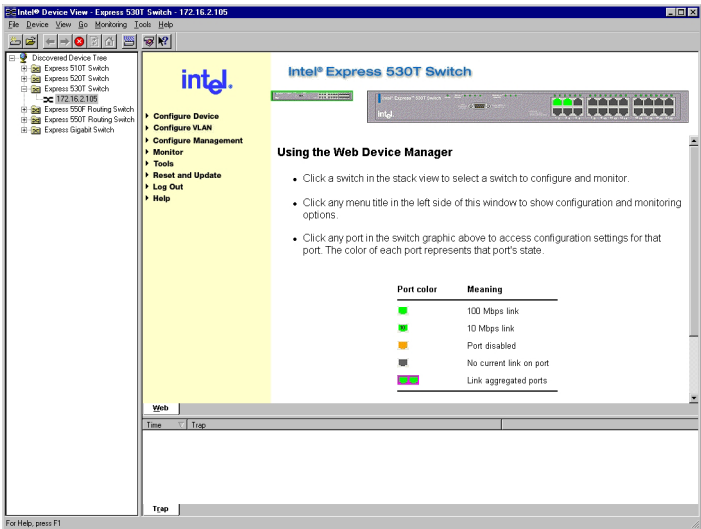
If the non-responding switch icon appears, you will not be able to manage the device in Intel Device View. If you're unable to ping the device or start a Telnet session, try accessing the switch's Local Management.

Managing a Switch

To manage the 530T switch, double-click the switch icon in the Device Tree. In the example shown below, the switch has been assigned an IP address of 124.123.122.3.



The 530T Web Device Manager appears in the Intel Device View window. For information on using the Web Device Manager, see Chapter 4.



For more information on using Intel Device View, refer to the program's online help or see the User Guide on the Intel Device View installation CD-ROM.

Viewing RMON Information

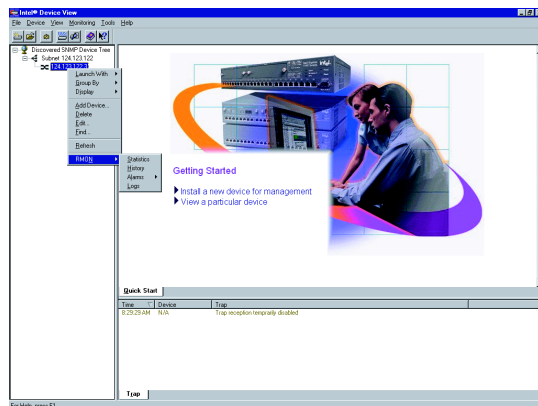
The remote monitoring (RMON) specification extends Simple Network Management Protocol (SNMP) functionality to look at traffic patterns on the network instead of merely looking at the traffic for an individual device. The following RMON groups are supported:

- **Group 1 (Statistics):** Monitors utilization and error statistics for each network segment (10Mbps or 100Mbps).
- **Group 2 (History):** Records periodic statistical samples from variables available in the statistics group.
- **Group 3 (Alarms):** Allows you to set a sampling interval and alarm thresholds for statistics. When a threshold is passed, the switch creates an event. For example, you might set an alarm if switch utilization exceeds 30%.
- **Group 9 (Events):** Provides notification and tells the switch what to do when an event occurs on the network. Events can send a trap to a receiving station or place an entry in the log table, or both. For example, when the switch experiences an RMON Event, it sends out an Alarm.

The switch also keeps a log that shows a list of the RMON Events and RMON Alarms that have occurred on the switch.

To view RMON statistics

- 1 Right-click the switch's icon in the Device Tree, then point to RMON.
- 2 Click the RMON option you want to view:



You can also access RMON features by using LANDesk Network Manager, or an SNMP application that supports RMON such as OpenView. For more information about using RMON to monitor the switch, refer to the Intel Device View Help.

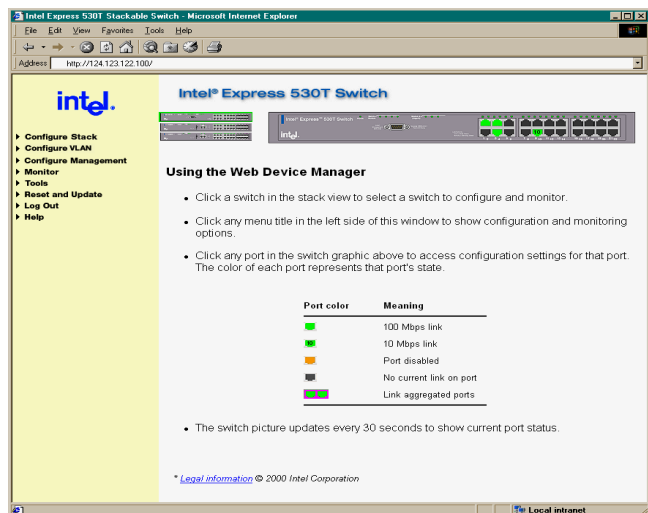
4

Using the Web Device Manager

Overview

The Web Device Manager, built into the Intel® Express 530T Switch, lets you use a Web browser to manage and monitor the switch. For example, you can use the Web Device Manager to configure the switch or individual ports, or to monitor traffic statistics and utilization.

This chapter covers the major management functions of the 530T. For additional information about using this interface, see the Web Device Manager Help.



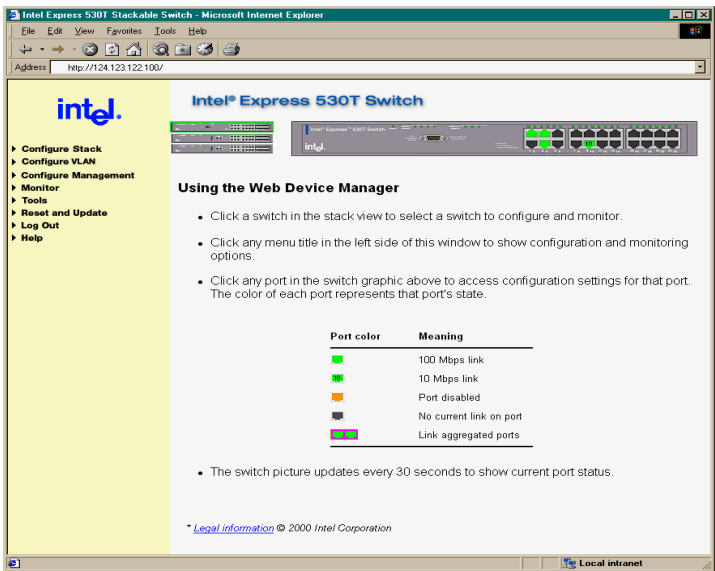
Accessing the Web Device Manager

NOTE

The default IP address assigned to the switch is 192.0.2.1. To access the switch with the default IP address, your workstation must be on the 192.0.2.0 subnet.

Alternatively, you can connect to the switch using Local Management and set an IP address that is on your network. Then you can access the Web Device Manager using the new IP address.

- 1 In the Location or Address field of your Web browser type the IP address of the switch. For example, to use the default IP address of the switch, type 192.0.2.1 in the Location or Address field and then press Enter.
- 2 When prompted, type your user name and password. By default, no user name or password is assigned. If you set a user name and password using Local Management, type those here.
- 3 Click OK. The Web Device Manager screen appears in your Web browser.



Navigating the Web Device Manager

Navigate between switches

On the switch stack graphic at the top of the page, click the switch you want to configure. The “active” switch is highlighted in green.

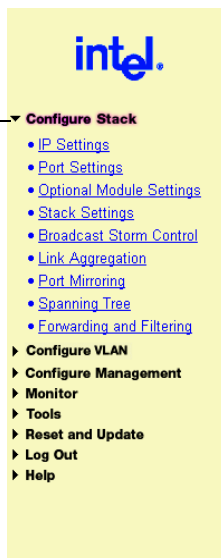
Click a switch in the stack to view or configure its settings.



Navigate between menus

- 1 On the left side of the Web Device Manager window, click a menu item (such as Configure Stack) to show the available options.
- 2 Click an option in the menu. The corresponding screen appears on the right side of your Web browser window.
- 3 To hide the options, click the menu item again.

Click a menu to view available options.



Using Management Screens

After you select an option from the navigation menu, the corresponding screen appears in the right side of the Web browser.

Switch faceplate graphic



A graphical representation of the switch’s faceplate appears at the top of the screen.

If the option you’re working with allows you to configure or monitor a specific port, you can change to another port by clicking it on the faceplate graphic.

Port color on the faceplate graphic indicates the status of the port.

Port Color	Meaning
Green	Port has a link at 100Mbps.
Green with “10”	Port has a link at 10Mbps.
Magenta outline	Ports are in a link aggregation.
Orange	Port is disabled.
Gray	No link.

Buttons

Configuration screens include four buttons on the bottom of each screen.

Button	Function
Submit	Applies the configuration settings on the current screen. Note: If you do not save the settings to the switch’s memory your changes will be lost when the switch is rebooted.
Reset	Clears any changes you made on the current screen and restores the currently applied settings.
Default	Applies factory defaults for this screen’s settings. When you log out, you can permanently save the new settings to the switch. Otherwise, they are lost upon the next reboot.
Help	Displays help for the current screen.

Configuring the Switch's IP Settings

Note: You must select Manual in the IP Assignment Method box before you can change the IP settings.

- 1 Click the Configure Stack menu and then click IP Settings. The IP Settings screen appears on the right side of the Web Device Manager window.

IP Settings

Enter the settings then click **Submit**. The new settings will take effect after the next switch reboot.

You can configure the IP settings only when the IP assignment method is Manual.

MAC Address:00-90-27-39-8D-AB

	Current Settings	New Settings
Assign IP:	Manual	Manual <input type="button" value="v"/>
IP Address	134.134.155.222	<input type="text" value="134.134.155.222"/>
Subnet Mask	255.255.255.0	<input type="text" value="255.255.255.0"/>
Default Gateway	134.134.155.251	<input type="text" value="134.134.155.251"/>

NOTE

Each stack of switches has one IP address.

- 2 To manually configure the IP settings, select Manual in the IP Assignment Method box. In the Change box, type the new IP address, subnet mask, and default gateway. If you have set up tag-based VLANs on the switch, you can specify the VID (VLAN ID) of the VLAN where the switch's SNMP management agent will reside.
- 3 To apply the changes, click Submit.
- 4 Click Save and Reboot for the new settings to take effect. Rebooting the switch temporarily interrupts network connectivity to the switch. Click Reboot Later if you want to reboot the switch later. The new IP settings do not take effect until the switch reboots.

Configuring a Port

You can use the Web Device Manager to enable or disable a port, and to change its speed, duplex, flow control, and priority settings.

To change port settings

- 1
- Click the Configure Stack menu and then click Port Settings. To access the Port Settings screen for each port, click the port you want to configure on the faceplate graphic.

Control Switch - Port 1 Settings

[Configure All Ports and Module in a Switch](#)

[View All Ports and Module in a Switch](#)

To configure a port in a different switch, use the stack view to select a switch. Enter the settings, then click Submit to apply the changes on this page. The flow control setting will take effect after the next switch reboot.

Link Status: 100Mbps/Full/FC-Off

Port State	Enabled
Speed/Duplex	Auto-Negotiate
Flow Control	Auto
Priority Queue	Default (Use Frame Priority Tag)

Note: This is the anchor port for a link aggregation. Any changes you make to this port's configuration will also affect any ports linked to it.

Submit

Reset

Default

Help

NOTE

If you change the flow control or IP settings, you must reboot the switch before the new settings can take effect.

- 2
- Click the options you want to change.
- **Port State:** Enable or disable the port.
 - **Speed/Duplex:** Set port speed to Auto-Negotiate, 10Mbps, or 100Mbps.
 - **Flow Control:** Enable or disable flow control.
 - **Priority Queue:** Set the priority queue for packets sent or received on this port.
- 3
- Click Submit.

Managing User Accounts

Create user accounts to give specific users read or write access to the switch through the Web Device Manager and Local Management. You can create a maximum of three accounts on the switch.

NOTE

The accounts and passwords you create with the Web Device Manager are the same accounts and passwords used to access Local Management.

To create a user account

- 1 Click the Configure Management menu and then click User Accounts. The first account you create must be an administrator.

User Accounts

User Name	Access
cyu	administrator
byoshi	user(view data only)
acalkins	user(view data only)

- 2 Click Add.

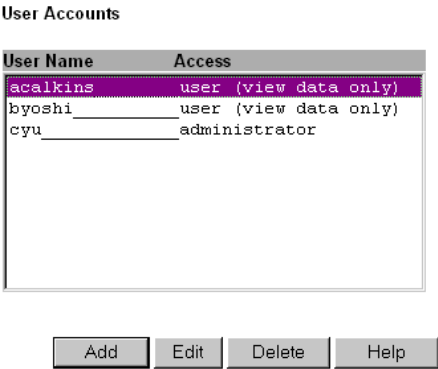
Add User

User Name :
 Password:
 Confirm Password:
 Access Level:

- 3 Type a user name in the User Name box. The username can be up to fifteen characters long and is case-sensitive.
- 4 The password can be up to fifteen characters long and is case-sensitive. Asterisks (*) appear on the screen as you type the password.
- 5 In the Confirm Password box, type the same password.
- 6 In the Access Level box click an access level. An administrator can view all settings and make configuration changes. A user can only view settings.
- 7 Click Submit.

To delete a user account

- 1 Click the Configure Management menu and then click User Accounts.
- 2 In the User Accounts screen, click the account you want to delete.



- 3 Click Delete.

If you delete the account you used to log in for this session, you can still use that account until you log out. If you delete the only user account on the switch, you can log in again using the default of no user name and no password.

Configuring VLANs

Virtual LANs, or VLANs, provide a way to create a logical network grouping without regard to physical location of the network nodes.

For more information about VLANs, refer to “Virtual LANs” in Chapter 2.

There are two main steps to set up a VLAN with the Web Device Manager:

- Set the switch’s VLAN operation mode.
- Configure the type of VLAN you selected.

NOTE

You can have only one operation mode (either port- or tag-based) active on the switch at a time.

To set the switch’s VLAN operation mode

- 1 Click the Configure VLAN menu and then click VLAN Operation Mode.
- 2 From the Current VLAN mode box, click the type of VLAN to set up.

VLAN Operation Mode

Select a VLAN mode, then click **Submit** to save changes and reboot the switch.

Current VLAN mode is: No VLAN (Default) No VLAN (Default) Port-based VLAN IEEE 802.1Q VLAN

Submit Reset help

You can set the 530T switch to use port-based or tag-based VLANs. See “Virtual LANs” in Chapter 2 for more information about VLAN types.

- 3 Click Submit.
- 4 The switch will automatically reboot. The 530T must be rebooted whenever you change its VLAN operation mode.

After the switch restarts, you can configure the type of VLAN that you selected.

NOTE

When the 530T is in a stack with 535T switches, the 530T is the control switch. The other switches are numbered in the management interface according to how they are plugged into the Stack Matrix Module.

- Member Switch 2 = Plugged into switch port 1
- Member Switch 3 = Plugged into switch port 2
- Member Switch 4 = Plugged into switch port 3

Port-based VLAN

You configure a port-based VLAN by first creating the VLAN and then adding participating ports. The switch can support up to 24 port-based VLANs. A port can be a member of only one VLAN; port-based VLANs cannot overlap.

To configure a port-based VLAN

- 1 Click the Configure VLAN menu and then click Port-based VLAN.
- 2 Click Add to create a new VLAN, or select a VLAN and click Edit to change its configuration.

Port-based VLAN Membership

To add a port to this VLAN, select it in the Available ports column and click Add. Ports that belong to another VLAN cannot be added.

After you have configured the VLAN settings, click **Submit** to apply the changes on this page.

VLAN Name:

Switch Unit :

Available ports		Member ports
1	<div>Add ></div> <div>< Remove</div>	Control Switch, Port 5
2		Member Switch 2, Port 10
3		Member Switch 3, Port 20
4		
5		
6		
7		
8		
9		
10		
11		
12		

☐ Enable IGMP Snooping for this VLAN

Submit

Reset

Default

Help

- 3 If you are creating a new VLAN, type a name in the VLAN Name box.
- 4 In the Switch Unit box, select a switch whose ports you want to add to the VLAN. You can include ports from any/all switches in a port-based VLAN.
- 5 In the Available ports box, select a port to add to the VLAN and click Add. Continue adding ports from each switch as necessary.
- 6 When you have finished adding ports, click Submit.

Tag-based VLAN

You configure a tag-based VLAN by configuring port membership and ingress/egress rules. It is important to note whether the devices in your VLAN support 802.1Q VLAN tags. If some of your devices don't support tagging, additional configuration may be necessary.

To configure a tag-based (IEEE 802.1Q) VLAN

- 1 Create a VLAN and assign member ports.
 - Click the Configure VLAN menu and then click Tag-based (IEEE 802.1Q) VLAN.
 - From the main Tag-based VLAN page, click Add to create a new VLAN. To modify an existing VLAN, click the VLAN name and click Edit.
 - If you are creating a new VLAN, type a name and VID (from 2 to 4094) to identify it.

Add Tag-Based (IEEE 802.1Q) VLAN

[Basic](#) [Port Settings](#) [Port VID](#)

Assign a name and ID number to the new VLAN.

VLAN Name: VID:

Switch Unit:

Add tagged ports to the VLAN and click Submit to apply the changes on this pages.

Available ports		Member ports
1	Add >	
2		
3	< Remove	
4		
5		
6		
7		
8		
9		
10		
11		
12		

☐ Enable IGMP Snooping for this VLAN

Next > Reset Help

- In the Switch Unit box, select a switch whose ports you want to include in the VLAN. You can include ports from any/all switches in a tag-based VLAN.
- To add a port to the VLAN, click the port in the Available ports box and click Add. To remove a port, click the port in the Member ports box and click Remove.
- The switch supports a maximum of 24 IGMP (Internet Group Multicast Protocol) Snooping sessions to manage broadcast traffic. If you want the VLAN to be part of an IGMP Snooping session, select the Enable IGMP Snooping check box.
- When you have finished adding ports, click Next.

2 Configure ports for egress (outbound) tagging.

- Ensure that the VLAN Name field displays the name of the VLAN you are configuring.
- Select Tag or Untag for each of the VLAN’s ports, to determine whether the switch removes (untags) tags before sending traffic out of each port.

NOTE

Select “Tag” when devices connected to the port support 802.1Q VLANs. Select “Untag” when devices connected to the port do not support 802.1Q VLANs.

If the VLAN members are from more than one switch, scroll down the screen to configure tagging for those ports.

- Click Submit.

Tag-based (IEEE 802.1Q) VLAN - Egress Port Tagging

Basic Port Settings Port VID

Enter the settings, then click Submit to apply the changes on this page.

VLAN Name: marketing VLAN ID: 50

Control Switch:

Port	Settings	Port	Settings	Port	Settings
1	Untag	9	N/A	17	N/A
2	Tag	10	N/A	18	N/A
3	N/A	11	N/A	19	N/A
4	N/A	12	N/A	20	N/A
5	N/A	13	N/A	21	N/A
6	N/A	14	N/A	22	N/A
7	N/A	15	N/A		
8	N/A	16	N/A		

1000Base-SX Module Port Settings

Port	Settings
1	N/A
2	N/A

- 3 Configure ports for handling untagged traffic.
 - From the main Tag-based VLAN page, click Port Settings.
 - On the Port Settings screen, you can set port-specific behaviors for processing VLAN traffic. To configure a specific port, click it in the faceplate graphic. To configure the same setting across all ports, click Configure All Ports and Module.

[Basic](#) [Port Settings](#) [Port VID](#)

[Configure All Ports and Module](#) [View All Ports and Module](#)

NOTE: If you change the Default PVID for this port, check that the port belongs to that VLAN. If the port is connected to a device that cannot process 802.1Q tags, the PVID must be a VLAN that includes the port. Otherwise, the switch will not forward untagged traffic coming into that port.

Enter the settings for all ports, then click Submit to apply the changes on this page.

All Ports

Default Port VID (Default VID for packets without an assigned VID)	<input type="text" value="1"/>
GVRP (For on-demand VLAN join / leave)	<input type="button" value="Disabled"/>
Ingress Filtering (Forward only packets with VID matching this port's configured VID)	<input type="button" value="Disabled"/>

Options include:

- **Default Port VID:** (This option is only available when you click Configure All Ports and Module. Sets the port VID (PVID) that is assigned to untagged traffic on a given port. For example, if port 10's default PVID is 100, all untagged packets on port 10 belong to VLAN 100. The default setting for all ports is VID 1.
- **GVRP (GARP VLAN Registration Protocol):** Allows automatic VLAN configuration between the switch and nodes.
- **Ingress filtering:** Allows incoming frames belonging to a specific VLAN to be forwarded if the port belongs to the same VLAN. Disabling this setting causes all frames to be forwarded, regardless of the port's VLAN membership.

Click Submit after you have changed the settings.

NOTE

When configuring link aggregation between two 530T switches, you must connect anchor port to anchor port, and member port to member port.

When a 530T is stacked with one or more 535T switches, you cannot aggregate ports that belong to different switches. The 530T supports up to four link aggregation groups (which includes the module ports), and each 535T in the stack supports up to three groups.

Link Aggregation

Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth between devices on the network, such as another switch or a server.

The anchor port is the base port in a link aggregation; it is the only port with configurable settings in the aggregation. All member ports in an aggregation take on the settings of the anchor port, this includes settings relating to VLANs and Spanning Tree.

Only consecutive ports, starting from the anchor port, can be grouped in a link aggregation. For example, ports 1, 2, and 3 are a valid link aggregation; ports 2, 4, and 7 are not.

On the Web Device Manager’s switch faceplate graphic, a link aggregation is shown with its ports outlined in magenta (pink).

To create a link aggregation

- 1 Click the Configure Stack menu, then click Link Aggregation.

Note: Connectivity is momentarily interrupted when changes are applied.

Anchor Port	Port Width	Group Name	Status
Port 1	2		Disabled
Port 7	2		Disabled
Port 15	2		Disabled
Module Port 1	2		Disabled

Submit

Reset

Default

Help

- 2 Choose the switch for which you want to configure link aggregation.
- 3 Choose the anchor port. Anchor ports are listed by number in the left column.
- 4 From the Port Width box, click the total number of ports (including the anchor port) to include in the link aggregation.
- 5 Type a name for the aggregation group.
- 6 Click Enable to make the group active.
- 7 Click Submit.

NOTE

Connectivity is momentarily interrupted when you apply changes.

Static MAC Addresses

The MAC address table stores all the MAC addresses that the switch records. The switch uses this table for forwarding traffic to specific devices, so it does not rely solely on broadcasting traffic to every port for communication.

There are two ways to add addresses to the MAC address table:

- 1 The switch can record addresses and add them dynamically. Dynamic entries remain in the table only while the associated node is active, and they are deleted if the node is inactive for longer than a specified period of time (age-out time; the default is 300 seconds).
- 2 You can manually add MAC addresses to the table. These are called static addresses because they remain in the table until you remove them, even if the associated node is inactive or taken off the network.

To add a static MAC address to the address table

- 1 Click the Configure Stack menu, then click Forwarding and Filtering.
- 2 Click Static MAC Addresses.
- 3 Click Add.

NOTE

To view the switch's address table, click the Monitor menu, click Advanced, then click MAC Address Table.

Add Static MAC Address

MAC Address:

(Do not use dashes when entering MAC addresses.)

VID:

Switch: Port Number:

NOTE

If you want to associate a MAC address with multiple VLANs, you must use tag-based VLANs.

- 4 In the MAC Address box, type the MAC address of a device on the network. Do not include hyphens.
- 5 If port-based or tag-based (IEEE 802.1Q) VLANs are set up on the switch, static MAC addresses are associated with specific VLANs. Type the VLAN name (port-based VLANs) or VID (tag-based VLANs) to associate with the MAC address.
- 6 In the Switch box, select the switch to whose ports you want to apply the filter.
- 7 In the Port number box, click a port number.

For the LX and SX optional modules, the port number is MP1.

- 8 Click Add.

Configuring Community Strings and Trap Receivers

A trap receiver is a computer on the network that is running an SNMP management application and receives messages sent by the switch. For example, the switch can send a trap to the trap receiver when it detects a change in port speed.

NOTE

These traps are supported by the switch:

- Power to the switch was cycled or reset.
- Link, speed, or other status changes on a port.
- Spanning Tree topology changes.
- A port is partitioned.
- Authentication failure.

To specify a trap receiver

- 1 Click the Configure Management menu and then click Community Strings and Traps.

Community Strings and Traps

Enter the settings, then click **Submit** to apply the changes on this page.

Community Strings

Read Community String	<input type="text"/>
Write Community String	<input type="text"/>

Trap Receiving Stations

IP Address	Status	Community String
<input type="text"/>	Enabled ▾	<input type="text"/>
<input type="text"/>	Enabled ▾	<input type="text"/>
<input type="text"/>	Enabled ▾	<input type="text"/>
<input type="text"/>	Enabled ▾	<input type="text"/>

- 2 In the IP Address box, type the IP address of the computer you want to use as a trap receiver. You can specify up to four trap receivers.
- 3 From the Status box, click Enabled.
- 4 In the Community Strings box, type the trap receiver’s SNMP application community strings. (The defaults are “public” for the Read Community String and “private” for the Write Community String.
- 5 Click Submit.

Monitoring Switch Activity

The Web Device Manager lets you view traffic, utilization, and error statistics for the switch and for individual ports. For more information on statistics, see “Port Traffic Statistics,” “Port Error Statistics,” and “Packet Analysis” in Chapter 5.

To view port statistics

- 1 Click the Monitor menu, and then click Port Statistics.
- 2 From the row of options below the page heading, click the option you want to view:
 - Traffic
 - Utilization Graph
 - Errors
 - Packet Analysis

Port 1 Statistics - Traffic

[Traffic](#) [Utilization Graph](#) [Errors](#) [Packet Analysis](#)

[Show in new browser](#)

Update Interval:

Link Status: 10Mbps/Half/Enabled (BackPressure)

Utilization: 65%

Last Seen MAC: 12-34-56-78-90-AE

Traffic in Bytes

Error-Free Bytes Sent	32234
Error-Free Bytes Received	1873
Total Bytes Received	876521

Traffic in Frames

Error-Free Frames Sent	3522
Error-Free Frames Received	4121
Total Frames Received	987628

Viewing/Changing Switch Information

You can view general information about the switch, such as its MAC address, firmware version, name, location, and contact person. Some of the fields can be updated; others are read-only.

- 1 Click the Configure Stack menu, and then click Stack Settings.

Stack Settings - Basic

Basic [Stack Information](#) [Advanced](#)

Enter the settings, then click **Submit** to apply the changes on this page.

Switch Name	<input type="text"/>
Location	<input type="text"/>
Contact	<input type="text"/>
MAC Address	00-90-27-39-8D-AB
Boot PROM version	v1.00.05
Firmware version	v1.00.10
Serial Number	6789ABCD

Submit	Reset	Default	Help
--------	-------	---------	------

- 2 The Switch Name, Location, and Contact fields allow you to provide additional information about the switch. You can type up to 40 characters in each field. After modifying the settings, click Submit.

Updating Switch Firmware

The Update Firmware screen sets up the switch to update its firmware from a TFTP server. The actual firmware update occurs while the switch is rebooting.

To update the switch's firmware

- 1 Click the Reset and Update menu, and then click Update Firmware.

Update Firmware

Enter settings, then click Submit to apply the changes on this page.

To start the firmware update, reboot the switch.

Update Mode:	<input type="text" value="Network"/>
TFTP Server Address:	<input type="text"/>
Firmware Update	<input type="text" value="Enabled"/>
File Name	<input type="text"/>

- 2 Select a mode from the Update Mode box.
 - If the switch uses a network connection for downloading the new firmware file, click Network.
 - If the switch uses a SLIP connection for downloading the new firmware file, click SLIP.
- 3 Type the IP address of the server that hosts the file in the TFTP Server Address box.
- 4 Click Enabled from the Firmware Update box.
- 5 In the File Name box, type the name of the firmware file.
- 6 Click Submit.

NOTE

If you don't have a TFTP server application, one is provided with Intel Device View (for Windows) and LANDesk® Network Manager.

The next time the switch reboots it downloads and installs the new firmware during the boot process. If you want to view this process, you must use a terminal program and be connected to the switch through the console port.

To update the switch's configuration file

The configuration file contains information and configuration settings specified by the network administrator. For more information on using configuration files, see “Upload Configuration Image File” in Chapter 5.

- 1 Click the Reset and Update menu and then click Change Configuration File.

Change Configuration File

Enter settings, then click Submit to apply the changes on this page.

To start using the new configuration file, reboot the switch.

Update Mode:	<input type="text" value="Network"/>
TFTP Server Address:	<input type="text"/>
File Download	<input type="text" value="Enabled"/>
File Name	<input type="text"/>

- 2 Select a mode from the Update Mode box.
 - If the switch uses a network connection for downloading the new configuration file, click Network.
 - If the switch uses a SLIP out-of-band connection (for example, via a serial port) for downloading the new configuration file, click SLIP.
- 3 Type the IP address of the server that hosts the file in the TFTP Server Address box.
- 4 Click Enabled from the File Download box.
- 5 In the File Name box, type the name of the configuration file.
- 6 Click Submit.

The new configuration settings are applied to the switch upon the next reboot.

Saving Configuration Changes and Logging Out

Each time you make configuration changes using the Web Device Manager, the switch immediately uses the new settings. However, when you log out of the Web Device Manager, you are prompted to permanently save the current configuration settings.

If you do not save the current configuration settings to the switch's permanent memory, the settings are lost upon the next switch reboot.

To save changes and log out

- 1 Click Log Out from the menu.

Log Out

The current configuration settings are lost upon the next switch reboot unless you save the changes to the switch's flash memory.

Click Save Now to permanently save the current configuration settings to the switch and close the Web browser window.

Click Do Not Save to close the Web browser window without saving the current configuration settings.



- 2 Click Save Now to save the current configuration settings. The Web browser window closes and you are successfully logged off of the Web Device Manager.

If you click Do Not Save, all current configuration settings are lost the next time the switch is rebooted.

5

Using Local Management

Overview

Another way to configure the switch is through the Local Management interface. Local Management provides the same functionality as the Web Device Manager using a text-based interface.

Accessing Management

You can access Local Management two different ways: connect directly to the switch's serial port, or through a Telnet session (using either an IP address you assign or the default IP address of 192.0.2.1).

Using the serial port

- 1 Use the enclosed null modem cable to connect the serial port of your PC to the serial port of the switch.
- 2 Start a terminal emulation program (such as HyperTerminal* in Windows* 2000). Use these communication parameters:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- No flow control

NOTE

When running HyperTerminal on Windows 2000, use the **Tab** and **Bksp** keys rather than the arrow keys to move between fields.

NOTE

You use the same user name and password to log into Web Device Manager and Local Management.


Press **Enter** to connect to the Local Management.

- 3 Log on to Local Management. By default, no password or user name is assigned. To assign them, see the section titled User Accounts in this chapter.

NOTE


Your workstation must be in the same subnet as the switch to Telnet to the switch.


Using Telnet

- 1 Open a Telnet application. In Windows 98 or Windows NT*, select Run from the Start Menu and then type: telnet .
- 2 From the Terminal menu, select Preferences. Make sure the emulation type is VT-100/ANSI and that VT100 arrows are enabled.
- 3 From the Connect menu, select Remote System. Enter the IP address of the switch and click Connect. (The default IP address is 192.0.2.1.)
- 4 Log on to Local Management. By default, no password or user name is assigned.

Logon Screen

Logon Screen

Enter username: []

Enter password: []


=====

Enter case-sensitive username. No username is assigned by default.

CTRL+R = Refresh

=====

Description

By default, no user name or password is assigned to the switch. Press  twice to log on to the Local Manager. User names and passwords can consist of any characters and can be up to fifteen characters in length. Remember that user names and passwords are also case-sensitive.

Navigation

The console menus provide a basic interface for configuring switch options. The text below the data provides navigation tips.

Help text at the bottom of the screen provides information on the selected item.

IP Settings

Switch MAC address: 00-90-27-39-00-10

Current Settings

Assign IP: BOOTP

IP address: 192.0.2.1

Subnet mask: 255.255.255.0

Default gateway: 0 .0 .0 .0

New Settings

Assign IP: <Manual>

IP address: [134.134.34.27]

Subnet mask: [255.255.255.0]

Default gateway: [134.134.34.251]

SUBMIT

Remember to save your changes to the switch's flash memory and reboot the stack for the new IP settings to take effect.







Submits the changes and returns you to the Configure Device screen.


CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

NOTE







When running HyperTerminal on Windows 2000, use the Tab key rather than the arrow keys to move between fields.

Screen legend

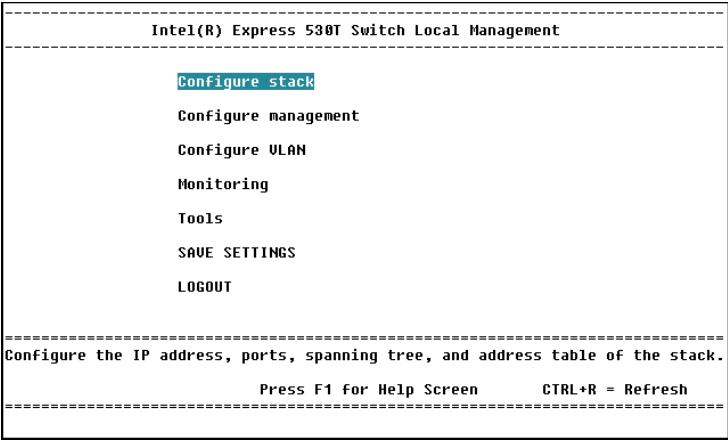
Use the     keys or the  and  keys to move between screen fields.

<Manual> Angle brackets indicate a toggle field. Use the  to toggle selections within the field. In this example, the options change between Manual, BOOTP (Boot Prom), and DHCP (Dynamic Host Configuration Protocol).

[255.255.255.0] Brackets indicate an input field. Select the field with the arrow keys and type the required information. By default, Local Management is in overstrike mode, which means it replaces existing characters as you type.

SUBMIT Any word in all caps is a button. Use the  key or the     keys to select the button, and press  to activate it.

Main Menu (Top Screen)



LOCATION

To return to the Main Menu at any time, press **Ctrl** **T**.

Description

The Main Menu is the starting point for all other Local Management screens. Use the **↑** **↓** arrow keys to choose an option and press **↵** **Enter** to display the screen.

Configure stack: Accesses menus to assign an IP address to the stack, change port settings, or configure advanced switch settings.

Configure management: Allows you to set SNMP traps and trap monitoring stations, administer user accounts, or update the switch's firmware.

Configure VLAN: Set up and administer VLANs on the switch.

Monitoring: Accesses menus to monitor traffic and activity at the port or switch level. They also provide information on network errors and collisions.

Tools: View the switch Trap/Event log, ping devices to check connectivity, save the current switch configuration to an image file on a server.

SAVE SETTINGS: Saves configuration changes to the switch's flash memory. Any changes not saved to memory are lost on the next reboot.

LOGOUT: Returns to the logon screen.

Configure Stack

Configure Stack	
IP settings	Port mirroring
Port settings	Link aggregation
Optional module settings	Broadcast storm control
Stack settings	
Spanning Tree Protocol	
Forwarding and filtering	
Configures IP address, subnet mask, and default gateway; or enables BOOTP/DHCP.	
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh	

LOCATION
Main Menu
 Configure Stack

Description

- IP settings:** Configures the switch's (stack's) IP address.
- Port settings:** Configures port speed, enables and disables ports, and displays link status.
- Optional module settings:** Configures the module's speed and duplex settings, enables and disables ports, and displays link status.
- Stack settings:** Sets stack's identification, displays detailed information about the switch hardware and firmware, and configures some advanced switch settings.
- Spanning Tree Protocol:** Configures Spanning Tree for the entire switch or individual ports.
- Forwarding and filtering:** Adds, removes, or locks the switch's address table, enables IGMP snooping, and sets filters for specific MAC addresses.
- Port mirroring:** Sends a copy of data from one port to another for monitoring and troubleshooting purposes.
- Link aggregation:** Combine ports on the switch to increase bandwidth.
- Broadcast storm control:** Configures ports to drop excessive broadcast traffic before it floods the network.

IP Settings

IP Settings

Switch MAC address: 00-90-27-39-00-1D

Current Settings

Assign IP: BOOTP

IP address: 192.0.2.1

Subnet mask: 255.255.255.0

Default gateway: 0 .0 .0 .0

New Settings

Assign IP: <Manual>

IP address: [134.134.34.27]

Subnet mask: [255.255.255.0]

Default gateway: [134.134.34.251]

SUBMIT

Remember to save your changes to the switch's Flash memory and reboot the stack for the new IP settings to take effect.

Submits the changes and returns you to the Configure Device screen.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu
Configure Stack
IP Settings

NOTE

The default IP address for the switch is 192.0.2.1

If the 530T is in a stack of switches, there is only one IP address.

Default VLAN for SNMP agent:
Port-based: DEFAULT_VLAN
802.1q-based: VID=1

Description

Switch MAC address: The unique hardware address assigned by Intel.

Current settings: The switch's current IP configuration.

New settings: Assign a new IP configuration to the switch.

- Assign IP:** Indicates if the switch will use a BOOTP or DHCP server to obtain an IP address dynamically, or if you will assign an address manually.
- IP address:** The IP configuration used by the switch. Use the IP address shown here to access the switch through Telnet or a ping test.
- Subnet mask:** Should match the mask for other devices on the network.
- Default gateway:** The IP address of the device that routes to different networks—typically, a router or routing server. Set this option to manage the switch remotely.
- VLAN or VLAN ID (port-based or tag-based VLANs only):** Specify a VLAN where the switch's SNMP management agent will reside. This option appears only when port-based and IEEE 802.1Q VLANs are active on the switch.

SUBMIT: Submits the changes and returns you to the Configure Device screen. You must save the changes to the switch's flash memory and reboot the switch for the new IP settings to take effect.

Port Settings

Port Settings					
Select switch: < Control >			Configure ports: < 1 to 12 >		
Port	State	Speed/Duplex	Flow Ctrl	Priority	Link:Speed/Duplex/Flow
1	<Enabled>	<100M/Full>	<Enabled>	<Frame>	10M/Half/Off
2	<Disabled>	<Auto>	Auto	<Frame>	-
3	<Enabled>	<100M/Half>	<Disabled>	<Frame>	100M/Half/Off
4	<Enabled>	<10M/Full>	<Enabled>	<Frame>	-
5	<Enabled>	<10M/Half>	<Enabled>	<Frame>	-
6	<Enabled>	<Auto>	Auto	<Frame>	-
7	<Enabled>	<Auto>	Auto	<Frame>	-
8	<Enabled>	<Auto>	Auto	<Frame>	-
9	<Enabled>	<Auto>	Auto	<Frame>	-
10	<Enabled>	<Auto>	Auto	<Frame>	-
11	<Enabled>	<Auto>	Auto	<Frame>	-
12	<Enabled>	<Auto>	Auto	<Frame>	-
Blocks the port from receiving or transmitting.					
CTRL+T = Main Menu (Top)		Esc = Previous screen		CTRL+R = Refresh	

LOCATION

Main Menu
Configure Stack
Port Settings

Description

Select switch: Press the **[Spacebar]** to select a switch to configure.

Configure ports: Press the **[Spacebar]** to select a range of ports to configure.

State: Press the **[Spacebar]** to toggle the field and disable or enable ports.

Speed/Duplex: Press the **[Spacebar]** to toggle the field's options and change the speed and duplex of the port. You can set the port to auto-negotiate speed, or to 10Mbps or 100Mbps at half- or full-duplex.

Flow Ctrl (Control): Press the **[Spacebar]** to enable or disable flow control.

Priority: Press the **[Spacebar]** to change the settings. The <Frame> setting reads the packet's 802.1p priority tag and handles it accordingly. The <Low> or <High> settings force the packet into one of two priority queues. Forcing a packet into a queue does not retag the packet.

Link: Indicates the port's current link status:

- **--** : No device link or port is disabled.
- **10M/100M**: The port's speed, either 10Mbps or 100Mbps.
- **Full/Half**: A device is connected at full- or half-duplex.
- **IEEE/BackP**: The type of flow control, either IEEE PAUSE frames or backpressure.
- **Partitioned**: Port was disabled due to a partition error.
- **Source mirror/Target mirror**: The port being mirrored and where the data is being sent.

Configure Optional Module

Configure Optional Module

Select switch: < Control >

Module A: 1000BaseT Module (2 ports) present

Module Port 1

State: <Enabled >

Speed/Duplex: <1000Mbps/Full>

Flow control: <Enabled >

Priority: <Frame >

Link (S/D/F): 1000M/Full/IEEE

Module Port 2

State: <Enabled >

Speed/Duplex: <100Mbps/Full>

Flow Control: <Enabled >

Priority: <Frame >

Link (S/D/F): 100M/Full/IEEE

Enables/disables the port.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu
Configure Stack
Optional Module...

NOTE

This screen is for Module A's settings; the Matrix Module is not configurable.

This screen also allows you to configure the Module A ports for any 535T switches in the stack.

1000SX and 1000LX modules connect at 1000Mbps, full-duplex only.

Description

Select switch: Press the **[Spacebar]** to select a switch.

Module A: Displays the type of module installed.

State: Press the **[Spacebar]** to toggle the field and disable or enable ports.

Speed/Duplex: Press the **[Spacebar]** to toggle the field's options and change the speed and duplex of the port. You can set the port to auto-negotiate speed or force to 100Mbps at half- or full-duplex (535T modules only).

Flow control: Press the **[Spacebar]** to enable or disable flow control.

Priority: Press the **[Spacebar]** to change the settings. The <Frame> setting reads the packet's 802.1 priority tag and handles it accordingly. The <Low> or <High > settings force the packet into one of two priority queues. Forcing a packet into a queue does not retag the packet.

Link: Indicates the port's current link status:

- :** Indicates no device link or port is disabled.
- 10M/100M/1000M:** The port's speed, either 10Mbps, 100Mbps, or 1000Mbps (535T modules only; 530T modules are 1000Mbps only).
- Full/Half:** A device is connected at full- or half-duplex.
- IEEE/BackP:** The type of flow control, either IEEE PAUSE frames or backpressure.
- Partitioned:** Port was disabled due to a partition error.
- Source mirror/Target mirror:** The port being mirrored and where the data is being sent.

Stack Settings

Configure Stack Settings

Name: [Switch 1, Engineering Dept.]

Location: [4th Floor, Building 2]

Contact: [John Adams, System Admin, 555-1212]

MAC address: 00-90-27-39-00-10

Boot PROM version: v1.00.15

Firmware version: v1.00.18

Serial number: 00000027

VIEW STACK INFORMATION

CONFIGURE ADVANCED SETTINGS

Sets a name for identification purposes.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

- Main Menu
- Configure Stack
- Stack Settings

NOTE

It's a good idea to write down both the firmware version and Boot PROM version, in case you need to contact Intel Customer Support.

Description

- Name:** The name of the switch, up to 40 characters long.
- Location:** The location of the switch, up to 40 characters long.
- Contact:** The contact person or phone number for the switch, up to 40 characters long.
- MAC address:** The unique hardware address assigned by Intel.
- Boot PROM version:** The version of the switch's boot code.
- Firmware version:** The version of the firmware installed on the switch. You can update this software through the Update firmware and configuration files screen.
- Serial number:** The hardware serial number for the switch.
- VIEW STACK INFORMATION:** Use this to view information about the control switch (530T) and any member switches (535Ts) in the stack.
- CONFIGURE ADVANCED SETTINGS:** Advanced switch settings such as port auto-partition and Head of Line blocking.

View Stack Information

View Stack Information	
Control switch:	Intel Express 530T Switch
Module A:	1000BASE-SX 2 port Module Present
Stack Matrix Module is present	
Hardware Version:	Rev. 2 (2)
Member 2 switch:	Intel Express 535T Switch
Module A:	1000BASE-FX 2 port MT-RJ Module Present
Hardware version:	Rev. 1 (2)
Member 3 switch:	Intel Express 535T Switch
Module A:	1000BASE-FX SC 1 port Module Present
Hardware version:	Rev. 1 (2)
Member 4 switch:	Not Present
Module A:	-----
Hardware version:	-----
Displays all switches and optional modules present in the stack.	
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh	

Description

The View Stack Information screen displays information about the control switch (535T) and any member switches (530T) that are in the stack.

Control switch: The name of the control switch. This is always Intel Express 530T Switch.

Module A: The type of module installed.

Stack Matrix Module: A message indicating whether or not the Matrix Module is installed.

Hardware version: The hardware version installed on each switch.

Member X switch: The module and hardware version for each member switch in the stack.

LOCATION

- Main Menu
 - Configure Stack
 - Stack Settings
 - View Stack...

NOTE

When the 530T is in a stack with 535T switches, the 530T is the control switch. The other ports are numbered according to how they are plugged into the Matrix Module.

- Member Switch 2 = Switch 1
- Member Switch 3 = Switch 2
- Member Switch 4 = Switch 3

Configure Advanced Switch Settings

```
-----
                        Configure Advanced Switch Settings
-----

Auto-partition capability on all ports: <Enable >
Head of Line (HOL) blocking prevention: <Enable >
High-priority packet service ratio: <10 high: 1 low>

=====
Sets how often to send high-priority packets before low-priority packets.
CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
=====
```

LOCATION

- Main Menu
- Configure Stack
- Stack Settings
- Configure Advanced...

Description

Auto-partition capability on all ports: If this option is enabled, the switch partitions the port when more than 61 collisions occur consecutively while receiving data. The first time the switch receives a good packet it then unpartitions the port. If a port is partitioned the switch can transmit data over this port, but not receive data.

Head of Line (HOL) blocking prevention: If this option is enabled it prevents the forwarding of data to a port that is blocked. Normally, when the switch sends traffic to a port it goes to the port’s transmit queue and then is sent out. If the port’s transmit queue is already busy trying to send out data, then the switch will place the waiting traffic in the buffer memory until the port is ready to send it out.

However, if the port’s transmit queue remains full, the switch fills up more of the buffer with traffic waiting to be sent on that port. HOL blocking works on the assumption that it is better to drop the traffic waiting in the buffer than to continue using more memory and impacting performance across all the ports.

High-priority packet service ratio: This option lets you determine how many high-priority packets are sent out by the switch before sending a low-priority packet. For example, a ratio of 8 high:1 low means that the switch will send out eight high-priority packets before sending out one low-priority packet.

Configure Spanning Tree Protocol

```
-----
                        Configure Spanning Tree Protocol
-----

Spanning Tree Protocol status: <Enabled >
Topology changes:          1
Time since change:         66 secs ago
Root MAC address:          00-00-80-15-77-05
Root path cost:            10
Root port:                 12

Switch priority:           [32768]
Hello time:                [99 ]
Max age:                   [99 ]
Forward delay:             [99 ]

CONFIGURE SPANNING TREE FOR PORTS
=====
Enables/disables Spanning Tree Protocol for the entire stack of switches.

CTRL+T = Top screen (Home)      Esc = Previous screen      CTRL+R = Refresh
=====
```

LOCATION

- Main Menu
- Configure Stack
- Spanning Tree Protocol

NOTE

Only once instance of Spanning Tree is supported per switch (or per stack).

Description

The IEEE 802.1D Spanning Tree Protocol specification prevents loops in a network by allowing only one active path between any two network devices at a time.

Spanning Tree status: Use the **[Spacebar]** to enable or disable support for the Spanning Tree Protocol, where the entire switch is a bridge for which you can set spanning tree parameters. (Note: If you are running 802.1Q VLANs, spanning tree must be enabled and will be turned on automatically by the switch.)

Topology changes: The number of times the spanning tree has changed its configuration.

Time since change: The elapsed time (since the last switch reboot) since the spanning tree last changed its topology (the paths used to get through the network).

Root MAC address, Root path cost, Root port: Information used by the root bridge in the same spanning tree as the switch.

Switch priority: Accepts a number from 0 to 65535 (default is 32768). The device with the lowest number becomes the root device (starting point for the spanning tree).

Hello time: Accepts a number from 1 to 10 seconds (default is 2 seconds). This is the time between transmissions of configuration BPDUs (Bridge Protocol Data Units) when the switch is, or is attempting to become, the root in the spanning tree.

Max age: Type a number from 6 to 40 seconds (default is 20 seconds). This is the maximum time that information from a configuration BPDU is used by the switch before it is discarded.

Forward delay: Type a number from 4 to 30 seconds (default is 15 seconds). This is the amount of time between port states when the spanning tree is changing its status from blocking to forwarding.

CONFIGURE SPANNING TREE FOR PORTS: Takes you to the screen where you can set spanning tree values for individual ports.

Configure Spanning Tree for Ports

Configure Spanning Tree Protocol for Ports							
Select switch: < Control >							
Port	STP State	Cost	Priority	Port	STP State	Cost	Priority
1	<Enable >	[10]	[128]	13	<Enable >	[10]	[128]
2	<Disable>	[10]	[128]	14	<Enable >	[10]	[128]
3	<Disable>	[10]	[128]	15	<Enable >	[10]	[128]
4	<Disable>	[10]	[128]	16	<Enable >	[10]	[128]
5	<Enable >	[10]	[128]	17	<Enable >	[10]	[128]
6	<Enable >	[10]	[128]	18	<Enable >	[10]	[128]
7	<Enable >	[10]	[128]	19	<Enable >	[10]	[128]
8	<Enable >	[10]	[128]	20	<Enable >	[10]	[128]
9	<Enable >	[10]	[128]	21	<Enable >	[10]	[128]
10	<Enable >	[10]	[128]	22	<Enable >	[10]	[128]
11	<Enable >	[10]	[128]	MP-1	<Enable >	[10]	[128]
12	<Enable >	[10]	[128]	MP-2	<Enable >	[10]	[128]
Enables or disables Spanning Tree for each port.							
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh							

LOCATION

Main Menu
 Configure Stack
 Spanning Tree Protocol
 Configure STP for...

Description

Select switch: The switch you want to configure for spanning tree.

STP State: Use the Spacebar to enable or disable each port to be active in the spanning tree.

Cost: Accepts a number from 1 to 65535 (default is 10). This value is used by the Spanning Tree Protocol to determine alternate routes in the network to forward traffic. The higher the cost of a port, the lower the chance of this port being used to forward traffic. When possible, assign a port a low cost if it is connected to a fast network segment.

Priority: Accepts a number from 0 to 255 (default is 128) to set the port's priority in the spanning tree. The higher the value, the lower the chance of this port being used as the root port. If two ports on the switch have the same priority value, the spanning tree uses the port with the lowest number. For example, the spanning tree would choose port 1 over port 4 if they both had the same priority setting.

Forwarding and Filtering

```
-----
                          Forwarding and Filtering
-----

Lock address table (stops learning): <No >
MAC address aging (sec): [300 ]
Configure IGMP snooping
Configure static MAC addresses (forwarding)
Configure port security
Configure MAC address filtering
Configure Ethernet multicast filtering

=====
Prevents the switch from learning addresses automatically.
CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
=====
```

LOCATION

- Main Menu
- Configure Stack
- Forwarding and Filtering

Description

Lock address table: Use the Spacebar to toggle field values. <Yes> prevents the switch from learning new MAC addresses. Any existing addresses that the switch has learned remain in the address table.

MAC address aging: Sets the time interval at which the switch scans its MAC address table to determine the age of entries.

Configure IGMP snooping: Sets Internet Group Management Protocols (IGMP) options for multimedia applications, such as desktop video conferencing, that use IP multicast addresses.

Configure static MAC addresses (forwarding): Allows permanent mapping between a network device and a port.

Configure port security: Configures the switch to allow the transmission of authorized traffic only over a particular port.

Configure MAC address filtering: Allows the switch to drop traffic from a specific source.

Configure Ethernet multicast filtering: Blocks or forwards traffic over each port for Ethernet (MAC-based) multicast groups.

Configure IGMP Snooping

```
-----
                        Configure IGMP Snooping (IP multicast filtering)
-----

IGMP Snooping state: <Enable >
IGMP Snooping age-out timer (sec): [999]

=====
Enable/Disable IGMP snooping for the switch stack.
CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
=====
```

LOCATION

- Main Menu
 - Configure Stack
 - Forwarding and Filtering
 - IGMP Snooping

NOTE

If tag-based (IEEE 802.1Q) or port-based VLANs are currently running and you want to enable IGMP snooping for any of the VLANs, you must enable IGMP snooping for each VLAN separately. The switch supports a maximum of 24 VLAN IGMP snooping sessions.

Description

IGMP Snooping (Internet Group Management Protocol) is a feature that allows the switch to forward multicast traffic intelligently. The switch “snoops” the IGMP query and report messages and forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

IGMP requires a router that learns about the presence of multicast groups on its subnets and keeps track of group membership. Multicasting is not connection oriented, so data is delivered to the requesting hosts on a best-effort level of service.

VLAN name (when port-based or tag-based VLANs are running): The VLAN for which IGMP snooping is enabled. You can also enable IGMP snooping for a VLAN in the Configure VLAN section.

IGMP snooping state: Use the Spacebar to enable or disable IGMP Snooping.

IGMP snooping age-out timer: Specify the acceptable time (in seconds) between IGMP queries since the switch last received an IGMP query from the multicast server. The default time is 300 seconds. A query allows the server to determine which network hosts are (or want to be) part of the IP multicast group, and are configured and ready to receive traffic for the given application.

Configure Static MAC Addresses

Configure Static MAC Addresses		
Modify Address Table	Static Entries	Switch/Port
Enter MAC: 000000000000	00A0C9680F90	Mem2/08
	00A000123456	Mem2/09
Select switch: < Control >	00A0C9680F98	Mem2/20
Select port: < Port 1 >	00A0C9681312	Mem3/15
	00A0C9681330	Mem3/18
ADD DELETE	00A0C968133F	Mem3/20
	00A0C9681341	Mem3/22
Total entries: 2001	00A0C9681481	Mem4/01
	00A0C96814E5	Mem4/06
	00A0C9681552	Mem4/11
	00A0C9681579	Mem4/21
	- More -	
Enter a MAC address on a port so it is never removed from the address table.		
Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh		

LOCATION

- Main Menu
 - Configure Stack
 - Forwarding and Filtering
 - Configure Static MAC...

Description

Static MAC addresses are MAC addresses that remain in the switch’s address table, whether the device is physically connected to the switch. After you define a static MAC address, it remains in the switch’s address table until you remove it.

Enter MAC: Type the MAC address you want to permanently add to the address table.

VLAN or VLAN ID (when port-based or tag-based VLANs are running): When VLANs are active on the switch you can define static MAC addresses for each VLAN. If port-based VLANs are active press the **Spacebar** to select a VLAN. If tag-based VLANs are active type the VLAN ID that the static MAC address will be assigned to.

NOTE

If tag-based or port-based VLANs are currently running, you must assign each static MAC address to a specific VLAN.

Select switch: Use the **Spacebar** to select the switch you want to configure.

Select port: Use the **Spacebar** to select a port on the switch where the switch forwards traffic.

ADD/DELETE: Use these buttons to add or remove a MAC address from the switch’s table.

Configure Port Security

Port Security

Select switch: < Control >

Port	Learning	Port	Learning	Port	Learning	Port	Learning
1	<Enable >	7	<Enable >	13	<Enable >	19	<Enable >
2	<Disable>	8	<Enable >	14	<Enable >	20	<Enable >
3	<Enable >	9	<Enable >	15	<Enable >	21	<Enable >
4	<Enable >	10	<Enable >	16	<Disable>	22	<Enable >
5	<Enable >	11	<Enable >	17	<Enable >	MP1	<Enable >
6	<Disable>	12	<Enable >	18	<Enable >	MP2	<Enable >

Secure a port: 1. Disable the port from learning any new MAC addresses.
2. Use the Configure Static MAC Addresses screen to define a list of MAC addresses that can use the secured port.

Enables or disables the port from learning new MAC addresses.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu
 Configure Stack
 Forwarding and Filtering
 Configure Port...

NOTE

You must first configure port security and then configure a static MAC address.

Description

Port security prevents unauthorized access of a port by “securing” a list of specific MAC addresses to a port. If the switch sees a MAC address that is not on the secured list, it discards the traffic.

To set port security from Local Management

- 1 From the Configure Device screen, select Forwarding and Filtering.
- 2 From the menu select Configure Port Security.
- 3 Press the **[Spacebar]** to select the switch you want to configure.
- 4 Select a port you want to secure. Press **[Spacebar]** in the Learning field to disable the port’s ability to learn new MAC addresses.
- 5 Press **[Esc]** to move up a level and select the Configure Static MAC Addresses screen.
- 6 Define a list of MAC addresses and assign them to the same port you secured in the Port Security screen.

To turn off port security

- 1 From the Configure Device screen, select Forwarding and Filtering. Select Configure Port Security from this menu.
- 2 Press the **[Spacebar]** to select the switch you want to configure.
- 3 Select the port on which you want to disable security. Press the **[Spacebar]** in the Learning field to disable security and allow the port to learn new MAC addresses.

Configure MAC Address Filter Table

Configure MAC Addresses Filter Table

Add a Filter

Enter MAC: [000000000000]

ADDDELETE

Total entries: 2031

Filtered Addresses

00902700A002
00A0C9680F90
00AA00123456
00A0C9680F98
00A0C9681330
00A0C9681481
00AA0C18FB90
00A980700C28
009068000346
005011000200
00C266110004
00B426002492
- More -

Type a MAC address to filter on the switch.

Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh

LOCATION

- Main Menu
 - Configure Stack
 - Forwarding and Filtering
 - Configure MAC...

NOTE

If tag-based (IEEE 802.1Q) or port-based VLANs are currently running, you must assign each MAC address filter to a specific VLAN.

Description

MAC address filtering allows the switch to drop unwanted traffic. The switch will drop any traffic when it sees the specified MAC address in either the source address or destination address of the incoming packet. For example, if your network is congested because of high utilization from a specific MAC address, you can filter all traffic transmitted from that address and restore network flow, while you troubleshoot the problem.

Enter MAC: Type the MAC address you want to filter.

VLAN/VLAN ID (when port-based or tag-based VLANs are running): If VLANs are active on the switch you can set MAC address filtering on a per VLAN basis. For port-based VLANs, press the **Spacebar** to select the name of VLAN. For tag-based VLANs, type in the VLAN ID where the MAC address belongs.

ADD: Press **Enter** to activate the filter and add the MAC address to the list.

DELETE: Press **Enter** to remove the filter for the specified MAC address.

Configure Ethernet Multicast Filtering

Configure Ethernet Multicast Filtering (802.1Q VLAN)

Create/Remove a Filter

Multicast address: [00AA00000000]
VLAN ID: [0025]

ADD DELETE

To create: Enter the address and
VID then select ADD

To remove: Enter the address and
VID then select DELETE

Modify a Multicast Filter

Select a filter from the
list to modify the settings

Current Filters	VLAN ID
C3A5E9680E90	0005
D2A3C9681330	0110
F0A1D968358E	0118

Use the arrow keys to select a multicast filter. Press Enter to edit.

Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh

LOCATION

- Main Menu
 - Configure Stack
 - Forwarding and Filtering
 - Ethernet Multicast...

NOTE

If tag-based (IEEE 802.1Q) or port-based VLANs are currently running, you must assign each multicast filter to a specific VLAN.

Description

Ethernet multicast filters allow you to define which ports can receive ethernet multicast traffic from a specific multicast MAC address. This is similar to IGMP snooping, except you define everything manually.

Multicast address: Type the MAC address to which you want to apply a filter.

VLAN/VLAN ID: If VLANs are active on the switch you can set Ethernet Multicast filtering on a per-VLAN basis. For port-based VLANs, press the **Spacebar** to select the name of VLAN. For tag-based VLANs, type in the VLAN ID where the multicast address belongs.

ADD: Press **Enter** to activate the filter and add the address to the list.

DELETE: Press **Enter** to remove the filter for the specified address.

Adding/Deleting a multicast filter

- 1 In the Multicast address field, type a multicast address.
- 2 If the switch is running tag-based or port-based VLANs, select a VLAN to locate the filter.
- 3 Select ADD using the arrow keys and press **Enter**.
- 4 To remove a filter, type in the MAC address in the Multicast field, select DELETE, and press **Enter**.

Ethernet Multicast Filtering (Ports)

Configure Ethernet Multicast Filtering

Select Switch: < Control >

Multicast address: C3A5E9680E90

Port	Action	Port	Action	Port	Action	Port	Action
1	<Forward>	7	<Block >	13	<Forward>	19	<Forward>
2	<Forward>	8	<Forward>	14	<Forward>	20	<Block >
3	<Block >	9	<Block >	15	<Block >	21	<Block >
4	<Forward>	10	<Forward>	16	<Forward>	22	<Block >
5	<Block >	11	<Forward>	17	<Block >	MP1	<Block >
6	<Block >	12	<Block >	18	<Block >	MP2	<Forward>

APPLY CHANGES

Sets the switch to forward or block traffic to this port.

Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh

Description

Select switch: Press the **Spacebar** to select a switch to configure.

Multicast address: Displays the multicast address you want to filter.

Action: Use the **Spacebar** to select whether to block or forward traffic to the selected port.

APPLY CHANGES: Applies the changes to the multicast filter once you have configured the ports.

Modifying a multicast filter

- 1 Under the Configure Ethernet Multicast Filter screen use the arrow keys to select an address from the list on the right side of the screen. Press **Enter**.
- 2 Decide which ports should receive the multicast traffic by using the **Spacebar** to set Forward or Block for each port.
- 3 Select **APPLY CHANGES** and press **Enter**. This activates the changes to the multicast filter and returns you to the previous screen.

LOCATION

Main Menu
 Configure Stack
 Forwarding and Filtering
 Ethernet Multicast...
 Multicast Filters...

Port Mirroring

Port Mirroring

This feature allows you to mirror one port to another for network monitoring and troubleshooting purposes.

Source switch: < Control >
Source port: < 1 >

Target switch: < Member 2 >
Target port: < 10 >

State: <Disabled>

Selects a port to mirror.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

- Main Menu
 - Configure Stack
 - Port Mirroring

CAUTION

Do not mirror traffic to a target port that is connected to network devices other than a protocol analyzer. Their behavior may be unpredictable.

If a port is part of an aggregated link, it cannot be configured as the target port for a port mirror. However, a port in an aggregated link can serve as the source port for a port mirror.

Description

Port mirroring is a useful diagnostic tool because it allows you to send a copy of the good Ethernet frames transmitted or received on one port to another port. On the second port you can attach a protocol analyzer to capture and analyze the data without interfering with the client on the original port.

Source switch: Use the Spacebar to select the switch you want to configure.

Source port: Use the Spacebar to select the port whose traffic you want to mirror.

Target switch: Use the Spacebar to select the switch you want to receive mirrored traffic.

Target port: Use the Spacebar to select a port to receive the mirrored traffic. This is a port to which you have connected a protocol analyzer.

State: Use the Spacebar to enable or disable the port’s mirror.

Link Aggregation

Configure Link Aggregation			
Select switch: < Control >			
Anchor Port	Width	Group Name	Status
Port 1	<6 ports>	[Engineering Department Server]	<Enabled >
Port 7	<8 ports>	[Site Web Server]	<Disabled>
Port 15	<8 ports>	[]	<Disabled>
Module Port 1	2 ports	[]	<Disabled>
Connectivity is momentarily interrupted when changes are applied.			
Configures the port width of the link aggregation group.			
Ctrl+T = Main Menu (Top) Esc = Previous screen Ctrl+R = Refresh			

LOCATION

- Main Menu
 - Configure Stack
 - Link Aggregation

NOTE

All custom settings for a port (including VLAN membership) are lost when you add that port to a link aggregation.

You cannot link aggregate ports from different switches in the stack.

Description

Link aggregation is a way of combining ports on the switch to increase the available bandwidth and provide redundancy. All ports in the aggregated link take on the characteristics of the anchor port. This means that if you set the anchor port to 100Mbps full duplex, all the ports aggregated to that anchor port will share the same setting.

Select switch: Use the Spacebar to set the switch you want to configure.

Anchor Port: This shows the first port in the link aggregation.

Width: Use the Spacebar to set the total number of (consecutive) member ports in the aggregated link. The minimum number of ports for an aggregated link is two, and the maximum is eight. The link aggregation width includes the anchor port.

Group Name: Assigns a name to the aggregated links for management or identification purposes.

Status: Use the Spacebar to enable or disable the aggregated link.

Broadcast Storm Control

Broadcast Storm Control - Port Settings					
Select switch: < Control >					
Port	Setting	Upper Threshold	Port	Setting	Upper Threshold
1	<Enabled >	[20]%	13	<Enabled >	[20]%
2	<Enabled >	[20]%	14	<Enabled >	[20]%
3	<Enabled >	[20]%	15	<Enabled >	[20]%
4	<Disabled>	[20]%	16	<Enabled >	[20]%
5	<Enabled >	[20]%	17	<Enabled >	[20]%
6	<Disabled>	[20]%	18	<Enabled >	[20]%
7A	<Enabled >	[20]%	19	<Enabled >	[20]%
8	-	-	20	<Enabled >	[20]%
9	-	-	21	<Enabled >	[20]%
10	-	-	22	<Enabled >	[20]%
11	-	-	MP1	<Enabled >	[20]%
12	-	-	MP2	<Enabled >	[20]%
Sets the threshold value for the broadcast traffic.					
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh					

LOCATION

- Main Menu
 - Configure Stack
 - Broadcast Storm Control

Description

This feature allows you to filter out broadcasts from faulty devices and prevent them from degrading network performance.

Select switch: Use the Spacebar to select the switch to configure.

Setting: Use the Spacebar to enable or disable broadcast storm control on this port.

Upper Threshold: Accepts a value from 1-20%. The default value is 20%. This control lets you set the threshold of broadcast traffic on a port (shown as a percentage of the port's total bandwidth) that will activate broadcast storm control. When the amount of broadcast traffic on the port exceeds the upper threshold, the port drops all broadcast traffic. When broadcast traffic falls down below the threshold the switch will automatically start forwarding broadcast traffic again.

Configure Management

```
-----
                        Configure Management
-----

Configure community strings and trap receivers

Administer user accounts

Update firmware and configuration files

Reset and console options

-----
Manages user names, passwords, and access levels.
CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
-----
```

LOCATION
Main Menu
Configure Management

Description

Configure community strings and trap receivers: Sets the switch's community strings and specify trap monitoring stations.

Administer user accounts: Use this menu to configure user accounts. You can add or delete users, update passwords, and change a user's access rights.

Update firmware and configuration files: Configures the switch's internal software and to specify the location of configuration files.

Reset and console options: Reboots the switch or changes the settings on the serial port. You can also use this menu to set the switch back to its factory defaults.

Community Strings and Trap Receivers

Community Strings and Trap Receivers

Community Strings

Current read community: [public]

Current write community: [private]

Trap Receiving Stations

Station IP Address	Community String	State
[124.123.122.50]	[private]] <Enabled >
[0.0.0.0]	[] <Disabled>
[0.0.0.0]	[] <Disabled>
[0.0.0.0]	[] <Disabled>

Sets the read community string. Use for security purpose.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu
Configure Management
Community Strings and...

NOTE

- The switch supports these traps:
- Power to the switch was cycled or reset.
 - Link, speed, or other status changes on a port.
 - Spanning Tree topology changes.
 - A port is partitioned.
 - Authentication failure.

Description

Use this screen to send alerts to PCs with SNMP management applications (such as OpenView*) installed.

- **Current read community:** Sets a password for viewing (not changing) the switch configuration. The string you define here must match the read community string defined in an SNMP application. The default read community string is “public.”
- **Current write community:** Sets a password for viewing and changing the switch configuration. The string you define here must match the write community string defined in an SNMP application. The default write community string is “private.”

Trap Receiving Stations: When an event occurs, the switch automatically alerts the SNMP management application by sending a trap to the SNMP management stations (for example, PCs) defined here.

- **Station IP Address:** The IP addresses of PCs with SNMP applications (such as Intel® Device View or LANdesk Network Manager) installed.
- **Community string:** Type a string for the trap that matches the community string defined in the SNMP management application. If you don’t define one, the default is “public.”
- **State:** Enables or disables sending of traps to the specified trap receiver.

User Accounts

User Accounts

Add Users/Change Passwords

Username: [123456789012345]

Old password: [*****]

Access Level: <Administrator>

New password: [*****]

Confirm password: [*****]

APPLY CHANGES

Modify Current Accounts

User Name	Access Level	Delete
123456789012345	<Administrator>	<N/A>
123456789012345	<Normal User >	<Yes>
123456789012345	<Administrator>	<No >

APPLY CHANGES

Type the user's name.

CTRL+T = Main Menu (Top)

Esc = Previous screen

CTRL+R = Refresh

LOCATION

Main Menu
 Configure Management
 Administer User Accounts

Description

Add Users/Change Passwords

- **Username:** By default, no username is assigned. Usernames can consist of any character and can be up to fifteen characters long. You can define three usernames.
- **Old password:** Used when changing the password of a current user. If this is a new account, you can skip over to the New password field. By default, no password is assigned.
- **New password:** Sets a new password for accessing Local Management. The one you specify here is used the next time you reset the switch or log out and log in on Local Management. Passwords are case-sensitive and can be up to fifteen characters long.
- **Confirm password:** Verifies the entry in the New password field.
- **Access level:** Use the Spacebar to determine a user's access rights. Administrators can make any changes to Local Management. All other users (categorized under Normal user) can view information but cannot make changes. To change a user's access rights, see Modify User Accounts.
- **APPLY CHANGES:** Select this button to save changes when adding users or changing passwords.

Modify User Accounts

Access level: Use the **[Spacebar]** to change access rights for the user.

Delete: The default value is <No>. To delete an account, use the **[Spacebar]** to change the value to <Yes>.

APPLY CHANGES: Saves changes when modifying or deleting user accounts.

How to Manage User Accounts

System Administrators can create up to three user accounts for managing the switch. You can also change the access rights for current users and delete user accounts. Make sure you always set up at least one Administrator account.

To create a user account

- 1 From the Main Menu, select Configure Management. Under this menu select Administer User Accounts and press **[Enter]**.
- 2 On the User Accounts screen, type the name of the new user in the Username field and press **[Enter]**.
- 3 Since this is a new user, press **[Tab ↹]** to skip the Old password field and go to the New password field.
- 4 Type the password for the new user and press **[Enter]**. Passwords are case-sensitive and can be up to eight characters long.
- 5 To confirm the new password, retype it in the Confirm new password field. Press **[Enter]**.
- 6 To select the access rights for the new use, press the **[Spacebar]**.
- 7 To save the information, press **[Tab ↹]** to select SAVE CHANGES (below the Confirm new password field) and press **[Enter]**. The new account appears in the list under Modify User Accounts.

To change a password

- 1 From the Main Menu, select Configure Management, press **↵ Enter**. Under this screen, select Administer User Accounts and press **↵ Enter**.
- 2 In the Username field, type the username of the account for which you want to change the password. Press **↵ Enter**.
- 3 Type the current password in the Old password field and press **↵ Enter**.
- 4 Type the new password in the New password field and press **↵ Enter**.
- 5 To confirm the password and retype it in the Confirm new password field, press **↵ Enter**.
- 6 To save the new password, press **Tab ↵** to select SAVE CHANGES (below the Confirm new password field) and press **↵ Enter**.

To modify a user's access level

- 1 From the Main Menu, select Configure Management, press **↵ Enter**. Under this screen select Administer User Accounts and press **↵ Enter**.
- 2 Press **Tab ↵** to select the account to be modified under Access Level.
- 3 Press the **Spacebar** to change the user's access rights. Users with Administrator access can make changes to the management configuration; users with Normal User access can view the configuration but cannot make changes.
- 4 To save changes, press **Tab ↵** to select SAVE CHANGES at the bottom of the screen and press **↵ Enter**.

To delete a user account

- 1 From the Main Menu, select Configure Management, press **↵ Enter**. Under this screen, select Administer User Accounts and press **↵ Enter**.
- 2 Select the account to be removed under Delete.
- 3 Press the **Spacebar** to toggle the field from <No> to <Yes>.
- 4 To remove the user account, press **Tab ↵** to select SAVE CHANGES at the bottom of the screen and press **↵ Enter**.

Update Firmware and Configuration Files

Update Firmware and Configuration Files

Software update mode: network

TFTP Server Address: [124.123.122.15]

Update Management Module Firmware:

Firmware update: <Disabled>

Firmware file name: [run_10.tfp]

Change Configuration File:

Config File download: <Disabled>

Config File name: [530txt.cfg]

Last TFTP server address: 124.123.122.15

REBOOT TO START UPDATE

Determines where switch should look for new firmware.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

- Main Menu
- Configure Management
- Update Firmware and...

NOTE

Check Intel’s Customer Support Web site for firmware updates to the 530T switch.

Description

Software update mode: Use the Spacebar to select whether to update the switch’s firmware over the network or through a SLIP connection.

TFTP server address: IP address of the server used as the TFTP server.

Update Management Module Firmware

- Firmware update:** Use the Spacebar to enable or disable the firmware update. When enabled, the switch searches for the TFTP server specified at the top of the screen and attempts to update the firmware.
- Firmware file name:** Path and filename of the firmware located on the server.

Change Configuration File

- Config file download:** Use the Spacebar to enable or disable the ability to download a configuration file. When this field is enabled, the switch searches the TFTP server specified at the top of the screen.
- Config file name:** Path and filename of the configuration file located on the server.

Last TFTP server address: The IP address of the last TFTP server accessed by the switch.

REBOOT TO START UPDATE: Starts the update process. The switch reboots and downloads the specified file.

Reset and Console Options

```

-----
Reset and Console Options
-----

Reset Option:
Reboot stack:  RESET NOW

Reset stack settings to factory defaults: <No >

Serial Port Settings
Port setting:   <Console>           Current setting: Console
Console timeout: <30 mins>         Current timeout: 60 mins

(*) Changes become effective on next switch reboot.

=====
Sets the timeout interval in 15 min increments. 0 min is no timeout.

CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
=====

```

LOCATION

Main Menu
Configure Management
Reset and Console Options

Description

Reset Option

- **Reboot stack:** Resets the stack. If you changed the IP configuration or login setting, the new settings take effect after you select this option.
- **Reset stack settings to factory defaults:** This clears any IP address or current changes and resets the stack back to its factory defaults. All counters are cleared and the switch starts sending BOOTP requests.

Serial Port Settings

- **Port setting:** Configures the switch's serial port for out-of-band (SLIP) management. Press the Spacebar to toggle the field from <Console> to <SLIP>. Settings take effect on the next reboot.
- **Console timeout:** Logs out a user after a period of inactivity. Settings are from 0-90 minutes in 15-minute increments. A setting of <0 mins> means no timeout. The default is 60 minutes.

Configure VLAN Operation Mode

```
-----
Configure VLAN Operation Mode
-----

This switch is currently operating in Default mode (no VLANs).

Select the type of VLAN: <Port-based VLAN >          APPLY

-->Choose a VLAN then select APPLY to make
the VLAN active. The switch automatically
saves the changes and reboots.

-----
Select the type of VLAN to run on the switch.
Ctrl+T = Main Menu (Top)      Esc = Previous screen      Ctrl+R = Refresh
-----
```

LOCATION

Main Menu
Configure VLAN
(if switch is in Default Mode)

Description

This screen allows you to activate or change the type of VLAN operating on the switch. If there are no VLANs active on the switch, this is the first screen displayed when you select Configure VLAN from the Main Menu. By default, VLANs are not active on the Express 530T switch so they must be turned on before you can start configuring them.

The Express 530T supports only a single type of VLAN operating at a time. However, you can have multiple VLANs of the same type.

Select the type of VLAN: Press **[Spacebar]** to change the type of VLAN on the switch. The 530T switch supports two types of VLANs: port-based and IEEE 802.1Q (tag-based) VLANs.

APPLY: Makes the changes to the VLAN active and reboots the switch. Note: To change between VLAN types the switch must be rebooted.

- 1 Select Configure VLAN from the Main Menu.
- 2 From the Configure VLAN menu, select VLAN Operation Mode.
- 3 Press **[Spacebar]** to change the type of VLAN on the switch. Press **[Enter]**.
- 4 Select the APPLY button and press **[Enter]**. This reboots the switch and changes the VLAN mode.

Configure Port-based VLANs

```
-----
                                Configure VLAN (Port-based)
-----

VLAN operation mode

Add a port-based VLAN

Edit/Delete a port-based VLAN

=====
Configures the type of VLAN operating on the switch.
CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
=====
```

LOCATION

Main Menu
Configure VLAN

NOTE

You can have a maximum of 24 port-based VLANs on the switch.

VLAN membership can span between the switches in a stack. (Ports from any switch in a stack can be members of a VLAN.)

Description

A port-based VLAN allows you to create multiple VLANs each with its own broadcast domain and member ports. For example, if port 5 is in VLAN_1 and port 10 is in VLAN_2 the two ports cannot communicate with each other even though they are part of the same switch. Ports can be members of only a single port-based VLAN. Any port that is not a member of a user-defined VLAN is a member of the DEFAULT_VLAN.

- VLAN operation mode:** Changes the type of VLAN operating on the switch, or disables VLANs entirely.
- Add a port-based VLAN:** Creates a port-based VLAN and adds ports to the VLAN.
- Edit/Delete a port-based VLAN:** Selects a VLAN to change port membership in the VLAN, or removes a VLAN from the switch.

Add a Port-based VLAN

Create a Port-based VLAN

ULAN name: [ENGR_ULAN]

Select switch: < Control >

Port	Member	Port	Member	Port	Member	Port	Member
1	<Yes>	7	<No >	13	<Yes>	19	<Yes>
2	<No >	8	<Yes>	14	-	20	<No >
3	<No >	9	N/A	15	-	21	<No >
4	<No >	10	<Yes>	16	-	22	<No >
5	<Yes>	11	<Yes>	17	-	MP1	<No >
6	<Yes>	12	N/A	18	<No >	MP2	<No >

APPLY

Select 'Yes' or 'No' to add or remove each port from the VLAN.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu

Configure VLAN

Add a Port-based VLAN

Description

VLAN name: This field allows you to assign a name to the VLAN. Names can consist of any character (no spaces) and be up to 12 characters long. After a VLAN is created the name cannot be changed. If you want to change the name you need to delete the VLAN, create a new one, and assign the ports to the new VLAN.

Select switch: Press the **Spacebar** to select a switch to configure.

Member: Determines which ports will participate in the VLAN being created. Ports can be members of only one port-based VLAN. Press the **Spacebar** to toggle the field for the following options:

- <Yes>: The port will be a member of the VLAN
- <No >: The port will not be a member of the VLAN.
- : The port is part of an aggregated link.
- N/A : The port is already participating in another VLAN. Ports can belong to only one VLAN.

APPLY: Select this button and press **Enter** to create the VLAN and activate the settings.

NOTE

Ports from any switch in the stack can be members of the VLAN; follow this procedure to add ports from each switch, on switch at a time.

To create a port-based VLAN

- 1 Select Configure VLAN from the Main Menu.
Note: Make sure the switch’s current VLAN operation mode is set to port-based VLAN. If another type of VLAN is running, refer to “Configure VLAN Operation Mode” in Chapter 5 to change the VLAN operation mode.
- 2 Select Add a Port-based VLAN and press **Enter**.
- 3 Type a name for the new VLAN and press **Enter**.
- 4 Select the switch whose ports you want to be members of the VLAN, using the **Spacebar** to toggle between switches.
- 5 Select ports to add to the VLAN by using the **Spacebar** to toggle the Member field to Yes.
- 6 Select the APPLY button and press **Enter**.

Edit/Delete a Port-based VLAN

Edit/Delete a Port-based VLAN		
=====		
Edit/Delete a VLAN	VLAN Name	Ports
=====	=====	=====
Action: <Edit >	DEFAULT_VLAN	10
	ENGR_VLAN	5
	MKT_VLAN	8
	MFG_VLAN	4
After choosing an action, select a VLAN from the list at the right and press Enter.		
=====		
Choose to edit or delete a VLAN.		
Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh		
=====		

LOCATION

- Main Menu
 - Configure VLAN
 - Edit/Delete a Port-based..
 - Edit VLAN

Description

Action: Delete a VLAN or change its port membership. Press the **Spacebar** to toggle Edit or Delete and then use the **Tab** or **→** keys to select a VLAN and press **Enter**. The DEFAULT_VLAN cannot be deleted from the switch.

VLAN Name: The names of existing port-based VLANs.

Ports: Total number of member ports in the specified VLAN.

Edit VLAN Membership (Port-based)

Edit VLAN Membership (Port-based)

VLAN name: [ENGR_VLAN]

Select switch: < Control >

Port	Member	Port	Member	Port	Member	Port	Member
1	<Yes>	7	<No >	13	<Yes>	19	<Yes>
2	<No >	8	<Yes>	14	-	20	<No >
3	<No >	9	<Yes>	15	-	21	<No >
4	<No >	10	<Yes>	16	-	22	<No >
5	<Yes>	11	<Yes>	17	-	MP1	<No >
6	<Yes>	12	N/A	18	<No >	MP2	<No >

APPLY

Select 'Yes' or 'No' to add or remove each port from the VLAN.

CTRL+T = Main Menu (Top)Esc = Previous screenCTRL+R = Refresh

LOCATION

Main Menu
Configure VLAN
Edit/Delete a Port-based...

Description

This screen is very similar to the VLAN creation screen. You can change the membership status of ports within the VLAN but you cannot change the name of the VLAN.

VLAN name: The name of the VLAN you are editing.

Select switch: Press the **[Spacebar]** to select a switch to configure.

Member: Determines which ports will participate in the current VLAN. Ports can be members of only one port-based VLAN. Press the **[Spacebar]** to toggle the field for the following options:

- **<Yes>:** The port will be a member of the VLAN.
- **<No >:** The port will not be a member of the VLAN.
- **-** : The port is part of an aggregated link.
- **N/A** : If this is displayed it means the port is already participating in another VLAN. Ports can belong to only one VLAN.

APPLY: Select this button and press **[Enter]** to activate the settings.

Configure IEEE 802.1Q VLAN

```
-----
                        Configure IEEE 802.1Q VLAN
-----

VLAN operation mode

Create an IEEE 802.1Q VLAN

Edit/Delete an IEEE 802.1Q VLAN

Configure port VLAN ID for untagged and priority-tagged traffic

GVRP and ingress filtering settings

=====
Configures the type of VLAN operating on the stack.
CTRL+T = Main Menu (Top)      Esc = Previous screen      CTRL+R = Refresh
=====
```

LOCATION
Main Menu
Configure VLAN

Description

VLAN operation mode: Changes the type of VLAN operating on the switch, or to disable VLANs entirely.

Create an IEEE 802.1Q VLAN: Creates a new 802.1Q VLAN and add ports to the VLAN.

Edit/Delete an IEEE 802.1Q VLAN: Changes port membership of an existing VLAN, or you can remove a VLAN from the switch.

Configure port VLAN ID (PVID) for untagged and priority-tagged traffic: Assigns a VLAN to incoming packets without a VID.

GVRP and ingress filtering settings: Sets port-level options for dynamic VLAN creation and packet filtering by VLAN.

Add an IEEE 802.1Q VLAN (Configure Port Membership)

Add an IEEE 802.1Q VLAN (Configure Port Membership)

Ulan name: [ENGR_VLAN] Ulan ID: [45] Allow IGMP snooping: <Yes>

Select switch: < Control >

Port	Member	Port	Member	Port	Member	Port	Member
1	<Yes>+	7	<No >	13	<Yes>	19	<Yes>
2	<No >	8	<Yes>	14	-	20	<No >
3	<No >	9	<Yes>	15	-	21	<No >
4	<No >	10	<Yes>	16	-	22	<No >
5	<Yes>+	11	<Yes>	17	-	MP1	<No >
6	<Yes>	12	<No >	18	<No >	MP2	<No >

NEXT --->

Select 'Yes' or 'No' to add or remove each port from the VLAN.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu
 Configure VLAN
 Create an 802.1Q VLAN

NOTE

Devices on the network must have the same VID as the VLAN to be on the VLAN and be able to communicate.

NOTE

A '+' next to the Member toggle indicates that the port is a member of more than one VLAN.

Description

VLAN name: This field allows you to assign a name to the VLAN. The name can consist of any character (no spaces) and be up to 12 characters long. Once a VLAN is created the name cannot be changed.

VLAN ID: Assign a unique ID number to the VLAN. This number will be used to identify all packets belonging to that VLAN. Type in a number from 2 to 4094. The DEFAULT_VLAN (created when you select a VLAN operation mode) is assigned a VID of 1.

Allow IGMP snooping: Press the **[Spacebar]** to determine if the switch will perform IGMP snooping on this VLAN. There are a maximum of 24 IGMP snooping sessions allowed.

Select switch: Press the **[Spacebar]** to select a switch to configure.

Member: Identifies which ports will participate in the VLAN being created. Press the **[Spacebar]** to toggle the field for the following options:

- <Yes>: The port is a member of the VLAN
- <No >: The port is not a member of the VLAN.
- : The port is part of an aggregated link.

NEXT: Select this button and press **[Enter]** to access the Add an IEEE 802.1Q VLAN (Configure Port Tagging) screen.

Add an IEEE 802.1Q VLAN (Configure Port Tagging)

Add an IEEE 802.1Q VLAN (Configure Port Tagging)

Ulan name: ENGR_VLAN

Ulan ID: 1234

Select switch: <Control >

Port	Action	Port	Action	Port	Action	Port	Action
1	<Tag >	7	-	13	<Tag >	19	<Tag >
2	-	8	<Untag>	14	-	20	<Tag >
3	-	9	<Tag >	15	-	21	<Tag >
4	-	10	<Tag >	16	-	22	<Tag >
5	<Tag >	11	<Untag>	17	-	MP1	<Tag >
6	<Tag >	12	-	18	-	MP2	<Tag >

<--- PREV APPLY

Select 'Tag' to tag traffic for this VLAN. Otherwise, select 'Untag'.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

- Main Menu
 - Configure VLAN
 - Create an 802.1Q VLAN
 - Add an 802.1Q VLAN...

Description

VLAN name: Displays the VLAN name assigned on the Add an IEEE 802.1Q VLAN (Configure Port Membership) screen.

VLAN ID: Displays the VLAN ID assigned on the Add an IEEE 802.1Q VLAN (Configure Port Membership) screen.

Select switch: Displays the switch that is being configured.

Action: Indicates whether the device connected to this port supports tagging (press Spacebar).

PREV: Returns to the Add an IEEE 802.1Q VLAN (Configure Port Membership) screen.

APPLY: Returns to the Configure IEEE 802.1Q VLANs screen.

NOTE

Determine which devices on your network support tag-based VLANs and which do not, before you start this procedure.

How to Configure 802.1Q VLAN

Setting up a 802.1Q VLAN is a two-step process. The first step is to create a VLAN on the switch and assign member ports. The second step requires you to make sure that tagging is set up properly for your attached devices. For devices that don't support tagging an extra configuration step is required.

Step 1: Create an 802.1Q VLAN and add ports

- 1 From the Main Menu, select Configure VLAN.

Note: Make sure the switch's current VLAN operation mode is set to IEEE 802.1Q VLAN. Refer to "Configure VLAN Operation Mode" in Chapter 5 to change the VLAN operation mode.

- 2 Select Create an IEEE 802.1Q VLAN and press **↵**.
- 3 Type a name for the new VLAN (no spaces) and press **↵**.
- 4 Type a VLAN ID and press **↵**. The ID number can be any number from 2 to 4094.
- 5 Determine if you want to allow IGMP Snooping on this VLAN. This is important since the switch can support more 802.1Q VLANs than the maximum of 24 IGMP snooping sessions available.
- 6 Press the **Spacebar** to display the switch you want to configure.
- 7 Select ports to add to the VLAN. Use **Spacebar** to toggle the Member field to Yes.
- 8 Select the NEXT button and press **↵**.

Step 2: Configure tagging for member ports

If the device on a particular port does not support tags, configure that port as untagged. This ensures that the switch removes tags from packets before they leave the switch for the device. If you configure a port as untagged, proceed to step 3 (Configure VLAN for untagged devices) when you are finished with step 2.

- 1 Press **Spacebar** to select Tag or Untag for each port that is a member of the VLAN.
- 2 Select the APPLY button and press **↵**.

If you configured any of the ports in the VLAN as Untagged, proceed to step 3 to configure ports for untagged devices and associate those ports with a PVID (port VLAN ID).

Step 3: Configure VLAN for untagged devices

Even if the device attached to the switch doesn't support 802.1Q tags it is still possible for the device to participate in the VLAN. When communicating with untagged devices the switch performs two functions:

First, the switch determines how to forward untagged traffic. For untagged traffic, the switch assigns a default VID to the incoming traffic from the untagged device. Normally, all untagged traffic received on the switch is assigned a VLAN ID=1 or the DEFAULT_VLAN. You can change this PVID to the VID of the VLAN you want the port to use.

Next, the switch strips 802.1Q tags before sending traffic to the untagged device. When the switch needs to send traffic from a port to an untagged device, it strips the 802.1Q tag, otherwise the untagged device may not understand how to process the VID tag.

Use the following steps to add an untagged device to an 802.1Q VLAN.

- 1** Ensure that the port is a member of the VLAN. Refer to the procedure in step 1 (previous page) to add a port to an 802.1Q VLAN.
- 2** From the Configure VLAN menu, select Configure VLAN ID for untagged and priority-tagged traffic and press **←Enter**.
- 3** Press the **Spacebar** to display the switch you want to configure.
- 4** Select the port where the untagged device is connected. For example, port 7.
- 5** Type the VID of the VLAN you want the port to belong to and press **←Enter**. This is the same ID number you entered in step 1.

By specifying a VID you set the switch to assign a particular VID to any incoming traffic it receives on that port.

Edit/Delete an IEEE 802.1Q VLAN

Edit/Delete an IEEE 802.1Q VLAN

Select an Action

=====

Action: <Edit >

After choosing an action, select a VLAN from the list at the right and press Enter.

VLAN Name

=====

DEFAULT_VLAN1

ENGR_VLAN5

MKT_VLAN10

MFG_VLAN15

CUST_SUPPORT20

=====

Choose to edit or delete a VLAN.

Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh

=====

LOCATION

Main Menu
 Configure VLAN
 Edit/Delete an 802.1Q...

Description

Use this screen to select a VLAN to edit the port membership in the VLAN or delete the VLAN entirely from the switch.

Action: Press the Spacebar to toggle between <Edit> and <Delete>, then select a VLAN from the list and press Enter.

VLAN name: The name of the VLAN you are configuring.

VLAN ID: A unique number assigned to identify an 802.1Q VLAN.

Edit an IEEE 802.1Q VLAN (Configure Port Membership)

Edit an IEEE 802.1Q VLAN (Configure Port Membership)

VLAN name: [ENGR_VLAN]

VLAN ID: [1234]

Allow IGMP snooping: <Yes>

Select switch: < Control >

Port	Member	Port	Member	Port	Member	Port	Member
1	<Yes>+	7	<No >	13	<Yes>	19	<Yes>
2	<No >	8	<Yes>	14	-	20	<No >
3	<No >	9	<Yes>	15	-	21	<No >
4	<No >	10	<Yes>	16	-	22	<No >
5	<Yes>+	11	<Yes>	17	-	MP1	<No >
6	<Yes>	12	<No >	18	<No >	MP2	<No >

NEXT --->

Select 'Yes' or 'No' to add or remove each port from the VLAN.

CTRL+T = Main Menu (Top)Esc = Previous screenCTRL+R = Refresh

LOCATION

- Main Menu
- Configure VLAN
- Edit IEEE 802.1Q VLAN

Description

- VLAN name:** Name of the VLAN you are editing or deleting.
- VLAN ID:** Assigns a unique ID number to the VLAN. This number will be used to identify all packets belonging to that VLAN. Type in a number from 2 to 4094.
- Allow IGMP snooping:** Press the **[Spacebar]** to determine if the switch will perform IGMP snooping on this VLAN. There are a maximum of 24 IGMP snooping sessions allowed.
- Select switch:** Press the **[Spacebar]** to select a switch to configure.
- Member:** Determines which ports are part of the VLAN being created. Press the **[Spacebar]** to toggle the field for the following options:
- <Yes>: The port will be a member of the VLAN.
 - <No >: The port will not be a member of the VLAN.
 - : The port is part of an aggregated link.

NOTE

A '+' next to the Member toggle indicates that the port is a member of more than one VLAN.

NEXT: Select this button and press **[Enter]** to access the Edit an IEEE 802.1Q VLAN (Configure Port Tagging) screen.

Edit an IEEE 802.1Q VLAN (Configure Port Tagging)

Edit an IEEE 802.1Q VLAN (Configure Port Tagging)

VLAN name: ENGR_VLANVLAN ID: 1234

Select switch: <Control >

Port	Action	Port	Action	Port	Action	Port	Action
1	<Tag >	7	-	13	<Tag >	19	<Tag >
2	-	8	<Untag>	14	-	20	<Tag >
3	-	9	<Tag >	15	-	21	<Tag >
4	-	10	<Tag >	16	-	22	<Tag >
5	<Tag >	11	<Untag>	17	-	23	<Tag >
6	<Tag >	12	-	18	-	24	<Tag >

<---PREVAPPLY

Select 'Tag' to tag traffic for this VLAN. Otherwise, select 'Untag'.

CTRL+T = Main Menu (Top)Esc = Previous screenCTRL+R = Refresh

Description

This screen allows the switch to manage outgoing packets that do not contain IEEE 802.1Q VLAN tags.

VLAN name: Displays the name of the VLAN you are editing or deleting.

VLAN ID: Displays the ID number of the VLAN. This number identifies all packets belonging to that VLAN.

Select switch: Press the Spacebar to select a switch to configure.

Action: Determines whether outgoing traffic from that port is untagged by the switch.

PREV: Returns you to the Edit an IEEE 802.1Q VLAN screen.

APPLY: Returns you to the Configure VLAN (IEEE 802.1Q) screen.

Configure VLAN ID for Untagged Traffic

Configure Port VLAN ID For Untagged and Priority-tagged Traffic

Select switch: < Control >

Port	PVID	Port	PVID	Port	PVID	Port	PVID
1	[1]	7A	[1]	13	[1]	19	[1]
2	[15]	8	-	14	[1]	20	[1]
3	[150]	9	-	15	[1]	21	[1]
4	[1500]	10	-	16	[1]	22	[1]
5	[1]	11	-	17	[1]	MP1	[1]
6	[1]	12	[1]	18	[1]	MP2	[1]

Assign a port VLAN ID (PVID) from 1-4094. Changes are applied immediately.
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

LOCATION

Main Menu
 Configure VLAN
 Configure Port VLAN ID...

NOTE

If ports are aggregated, the letter A appears next to the anchor port, and the member ports do not display any data.

Description

This screen helps the switch manage incoming packets that do not contain IEEE 802.1Q VLAN tags or priority-tagged traffic (packets with a VID of zero). This is an ingress rule only; it does not apply to outbound traffic.

Untagged traffic is normally assigned to VLAN 1 (the DEFAULT_VLAN), which includes all ports on the switch. However, if you don't want to send untagged traffic on a specific port to the default VLAN, you can assign a different PVID.

For example, if you set a port's PVID to 5, all untagged traffic on the port will be assigned to VID 5—even if the port does not belong to that VLAN.

PVID: Type the VID of the existing 802.1Q VLAN where you want to send untagged traffic.

APPLY: Select this button and press **Enter** to apply changes on this page.

GVRP and Ingress Filtering Settings

GVRP and Ingress Filtering Settings		
Select switch: < Control > Configure ports: < 1 to 12 >		
Port	GVRP	Ingress Filtering
1	<Disabled>	<Disabled>
2	<Disabled>	<Disabled>
3	<Disabled>	<Enabled >
4	<Enabled >	<Enabled >
5	<Disabled>	<Disabled>
6	<Disabled>	<Disabled>
7	<Disabled>	<Disabled>
8	<Disabled>	<Disabled>
9A	<Enabled >	<Enabled >
10	-	-
11	-	-
12	-	-
Configures the switch to allow dynamic VLAN configuration on this port.		
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh		

LOCATION

Main Menu
 Configure VLAN
 GVRP and Ingress...

NOTE

In order for GVRP to work, the port must be connected to another switch that supports GVRP.

Description

Select switch: Use the Spacebar to select a switch to configure.

Configure ports: Use the Spacebar to toggle the range of ports that you can configure.

GVRP: Allows the switch to create VLANs dynamically. Use the Spacebar to toggle the action for each port. Options are:

- **<Enabled>:** The switch monitors traffic on this port for GVRP requests from network nodes. If a GVRP-enabled device sends a request to this port, the switch creates a VLAN dynamically and adds the requesting device to the new VLAN. This is the default setting.
- **<Disabled>:** The switch ignores GVRP requests in incoming packets on this port.

Ingress Filtering: Lets the switch filter incoming packets based on VLAN membership. Use the Spacebar to toggle the action for each port. Options are:

- **<Enabled>:** Incoming packets belonging to a specific VLAN are forwarded only if the port belongs to that VLAN. This is the default setting.
- **<Disabled>:** All packets coming into the port will be forwarded, regardless of the port's VLAN membership.

Monitoring (Network Statistics)

----- Network Monitoring -----
Switch stack overview
Port traffic statistics
Port error statistics
Packet analysis
IGMP snooping status
Browse address table
VLAN and GVRP status
=====
Displays switch statistics.
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh
=====

LOCATION
Main Menu
Monitoring

Description

Switch stack overview: An overview of all ports on the switch.

Port traffic statistics: Port traffic statistics and utilization.

Port error statistics: Port error statistics.

Packet analysis: Traffic per port by packet size and type.

IGMP snooping status: The active IP multicast groups detected by the switch.

Browse address table: The entries in the switch’s address table by port or MAC address.

VLAN and GVRP status: The status for static and dynamic tag-based (IEEE 802.1Q) VLANs. This option is available only when the switch is running 802.1Q VLANs.

Switch Stack Overview

Switch Overview							
Switch: < Control >				Update interval:<1 min>			
Port	Tx/sec	Rx/sec	% Util.	Port	Tx/sec	Rx/sec	% Util.
1	2154	21546	12	12	5310	5601	2
2	87654	4657878	23	13	0	0	0
3	79456321	397943215	34	14	0	0	0
4	0	0	0	15	0	0	0
5	0	0	0	16	14590	3657	10
6	0	0	0	17	7345	454687	1234
7	78761	12457	15	18	1256	3589	9
8	24685	7456	5	19	0	0	0
9	8798165	2478975	22	20	0	0	0
10	0	0	0	21	0	0	0
11	0	0	0	22	69855321	8965323	45
Module 0							
1	698523	245687	25	2	3698	1589	5
Sets the polling interval.							
CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh							

LOCATION

- Main Menu
- Monitoring
- Switch Stack Overview

Description

This screen provides a quick overview of activity on the stack. The information is displayed per switch. The screen displays the traffic sent and received for each port on the switch, including any optional modules, and the percent utilization for that port.

Switch: Press the Spacebar to select a switch to view.

Update interval: Press the Spacebar to select the time period between updates. For example, an Update interval of 5 sec means Local Management collects and displays information from the switch every five seconds.

Tx/sec or Rx/sec: The current rate of good frames that were transmitted or received by the port.

% Utilization: The percentage of Ethernet bandwidth (10Mbps, 100Mbps, or 1000Mbps) used by the device attached to that port.

Port Traffic Statistics

Port Traffic Statistics				
Switch: < Control >		Select port: < 1-4 >		Update interval: < 2 sec >
Port	1	2	3	4
Speed/Duplex	10Mbps/Half	100Mbps/Half	10Mbps/Full	100Mbps/Half
% Utilization	8	15	3	6
Bytes received	169608	501057	1397353	490297
Bytes sent	1150987	20882516	65497213	20884076
Frames received	2772	14479	43765	14473
Frames sent	2111	7264	21711	7171
Total bytes recv.	169608	501057	1397378	490297
Total frames recv.	2215	7264	21989	7171
Last seen MAC	00A0C9A3727B	00A0C96804E5	00A0C96814CB	00A0C9681481
Selects a group of ports to display traffic statistics.				
CTRL+T = Main Menu Esc = Previous screen C = Clear counters CTRL+R = Refresh				

- LOCATION
- Main Menu
 - Monitoring
 - Port Traffic Statistics

Description

- Switch:** Press the `Spacebar` to select a switch to view.
- Select port:** Selects the range of ports to view. Statistics are displayed four ports at a time. Press the `Spacebar` to toggle between port numbers and the optional module. The example shows ports 1-4 on a 24-port switch.
- Update interval:** Press the `Spacebar` to select the time period between updates. For example, an Update interval of 5 sec means Local Management collects and displays information from the switch every five seconds.
- Speed/Duplex:** The current connection status of the port.
- % Utilization:** The percentage of Ethernet bandwidth (10Mbps, 100Mbps, or 1000Mbps) used by the device attached to that port.
- Bytes received:** The number of bytes (octets) contained in error-free frames. This includes octets in unicast, broadcast, or multicast frames and packets whose destination address is mapped to the receiving port. It also includes octets in packets dropped because of full buffers, spanning tree, disabled ports, no link, or empty distribution list.
- Bytes sent:** The number of error-free bytes (octets) sent over this port.

Frames received: The number of frames detected without errors. Includes unicast, broadcast, or multicast frames and frames whose destination address is mapped to the receiving port. It also includes frames dropped because of full buffers, spanning tree, disabled ports, no link, or empty distribution list.

Frames sent: The number of frames sent over this port without errors.

Total bytes rcv. (received): The number of bytes (octets) contained in all frames received by this port. This counter reflects all bytes received on the port. This includes bytes contained in frames that contain errors, dropped frames, frames whose destination address is mapped to the receiving port, and frames that were not forwarded through the switch.

Total frames rcv. (received): This counter reflects all frames received on the port. This includes frames that contain errors, dropped frames, frames whose destination address is mapped to the receiving port, and frames that were not forwarded through the switch.

Last Seen MAC: Displays the MAC address of the last device that sent packets over this port. For a MAC address to appear in this field, the device must have sent at least one packet to the switch.

Port Error Statistics

Port Error Statistics				
Switch: < Control >		Select port: < 1-4 >		Update interval:<1 min >
Port	1	2	3	4
Speed/Duplex	10Mbps/Half	10Mbps/Full	-	-
CRC error	32	0	0	0
Oversize Frames	5	12	0	0
Fragments	120	8	0	0
Jabber	0	0	0	0
Late collision	0	0	0	0
MAC Rx error	0	0	0	0
Dropped Frames	10	3	0	0
Undersize frames	7	2	0	0
Total errors	174	25	0	0
Collisions	25	120	0	0

=====

Selects a group of ports to display statistics.

CTRL+T = Main Menu Esc = Previous screen C = Clear counters CTRL+R = Refresh

=====

LOCATION

Main Menu

Monitoring

Port Error Statistics

Description

Switch: Press the `Spacebar` to select a switch to view.

Select port: The range of ports to view. Statistics are displayed four ports at a time. Press the `Spacebar` to toggle between port numbers and the optional module. The example shows ports 1-4 on a 24-port switch.

Update interval: Press the `Spacebar` to select the time period between updates. For example, an Update interval of 5 sec means Local Management collects and displays information from the switch every five seconds.

Speed/Duplex: The current connection status of the port.

CRC error: The number of valid length frames that had a bad Frame Check Sequence (FCS).

Oversize frames: The number of frames exceeding the maximum allowed frame size but are otherwise valid Ethernet frames (good CRC).

Fragments: The number of frames that are less than 64 bytes; this number includes frames without a start-of-frame delimiter. A fragmented frame also has an invalid CRC.

Jabber: Indicates that a device (such as a faulty NIC) on the network is sending improper electrical signals. Because Ethernet uses electrical signaling to determine whether it can transmit, a jabber condition can halt all traffic on a segment.

Late collision: The number of collisions detected after the allowable detection period. This usually occurs in networks where cables are longer than the IEEE specification.

MAC Rx error: The number of received packets containing Rx Error events.

Dropped frames: The number of frames dropped by this port since the last switch reboot.

Undersize frames: The number of frames detected that are less than the minimum permitted frame size of 64 bytes and have a good CRC. Undersize frames usually indicate collision fragments, a normal network event.

Total errors: The total number of errors detected since the last switch reboot. Total errors include everything listed in this error table.

Collisions: A collision occurs when two devices try to transmit at the same time. This counter tracks the number of times packets have collided on this port. Collisions are normal in an Ethernet network and tend to increase as network utilization rises. Therefore, an increase in collision rate without an increase in network utilization might indicate a problem.

Packet Analysis

Packet Analysis									
Switch: < Control >			Select port: < 1 >			Update interval:<1 min >			
Length	Frames	Frames/sec				Frames	Frames/sec		
64	128133	22456							
65-127	188768	5464888				Unicast Packets			
128-255	134005	23449	RX	17560		29			
256-511	457162	235678	TX	14330		6			
512-1023	3003	13598984				Multicast Packets			
1024-Max	567	2135	RX	139401		23			
			TX	0		0			
						Broadcast Packets			
			RX	706034		3			
			TX	26987		0			
Selects a port for which to display statistics.									
CTRL+T = Main Menu Esc = Previous screen C = Clear counters CTRL+R = Refresh									

LOCATION
Main Menu
Monitoring
Packet Analysis

Description

This screen displays a breakdown of the traffic received on a port by size and type of frame.

Switch: Press the Spacebar to select a switch to view.

Select port: Selects the port to view. Statistics are displayed one at a time. Press the Spacebar to toggle between the ports and the optional module.

Update interval: Press the Spacebar to select the time period between updates. For example, an update interval of 5 sec means the switch collects and displays information every five seconds.

Length: Indicates the number of frames received of different lengths. This also includes dropped frames and frames whose destination address is mapped to the receiving port. It does not include frames that contain errors.

Frames

- **Unicast:** The number of good unicast frames received and transmitted on this port. Unicast frames are sent from one network node to another network node.
- **Multicast:** The number of good multicast frames received and transmitted on this port. Multicast frames are sent from one node to multiple nodes on the segment.
- **Broadcast:** The number of good broadcast frames received and transmitted on this port. Broadcast frames are sent from one network node to all nodes on a segment.

IGMP Snooping Status

IGMP Snooping Status	
IGMP snooping: Enabled	Age-out timer: 999
Select multicast group: 999.999.999.999	
MAC address: 00-AA-00-12-34-56	
Queries: 10	
Reports: 20	
Select switch: < Control >	
Ports: 1, 2, 3, 4, 5, 6, 7, 8	
Use the N and P keys to display information about an IP multicast group.	
Selects the switch for which to display information.	
Esc = Previous screen N = Next Group P = Prev Group CTRL+R = Refresh	

LOCATION

Main Menu
Monitoring
IGMP Snooping Status

Description

This screen displays the active multicast groups detected by the switch. The switch uses these groups for filtering purposes when you enable IGMP snooping.

VLAN: Displays the name of the VLAN with IGMP snooping enabled. This field only appears when port-based or tag-based VLANs are active on the switch.

IGMP snooping: The snooping status (enabled or disabled).

Age-out timer: The time the switch waits between IGMP queries.

Select multicast group: The IP address of the multicast group.

MAC address: The MAC address of the multicast group.

Queries: The number of IGMP requests sent from the IGMP multicast server or router to individual network hosts.

Reports: The number of notifications sent from each host to the server, signifying that the host is still (or wants to be) part of the multicast group.

Select switch: Press the Spacebar to select a switch to view.

Ports: The ports on the switch that have devices belonging to the selected multicast group.

Use the **N** (next group) and **P** (previous group) keys to display the status of different IP multicast groups on the switch.

Browse Address Table

```

=====
Browse Address Table
=====
Filter: <Switch/Port>      Switch: < Control >      Port number: < 2 >
Total addresses in table: 10029
DISPLAY
=====
Sw/Port  MAC Address      Learn      Sw/Port  MAC Address      Learn
1/2      0002B3002140     Dynamic    1/2      0090271EF390     Dynamic
1/2      0002B3002162     Dynamic    1/2      00902731C2B0     Dynamic
1/2      0002B3002A7E     Dynamic    1/2      00902731C2B3     Dynamic
1/2      0004AC661DC5     Dynamic    1/2      0090273925A6     Dynamic
1/2      0004AC661DF2     Dynamic    1/2      009027394026     Dynamic
1/2      001011477FFB     Dynamic    1/2      0090273E1140     Static
1/2      0030B6309043     Dynamic    1/2      0090273E1148     Static
1/2      0060F32088D4     Dynamic    1/2      0090273E2907     Static
1/2      0090270413AE     Dynamic    1/2      0090273E4B95     Dynamic
1/2      00902704141B     Dynamic    1/2      009027460BD5     Dynamic
1/2      0090270622C0     Dynamic    1/2      00902757D731     Dynamic
      - More -
=====
Specify to search table by MAC address or switch.

Esc = Previous screen      N = Next Page      P = Prev Page      CTRL+R = Refresh
=====

```

LOCATION

Main Menu
Monitoring
Browse Address Table

Description

This screen allows you to sort through the switch's MAC address table and view the addresses the switch has recorded. The switch uses this table forwarding traffic so it doesn't broadcast traffic over every port. You can choose to search this table by MAC address or port.

VLAN (port-based)/VLAN ID (tag-based): When the switch is running port-based or tag-based VLANs, the address table associates MAC addresses with specific VLANs. Use the **[Spacebar]** to select a VLAN.


Filter: Press the **[Spacebar]** to select how to view the address table. You can sort this table by <MAC address> or by <Switch/Port>.

Enter MAC address: Use this field to search for a specific MAC address in the switch's table.

Switch: Press the **[Spacebar]** to select a switch to view.

Port number: Use the **[Spacebar]** to select a port. This displays the MAC addresses seen on the specified port. This search is useful for monitoring which ports a device is using, or which devices are using one port.

Total addresses in table: The total number of addresses recorded by the switch. This number includes addresses that have been entered manually into the switch through the Static MAC Addresses screen.

DISPLAY: After you have entered in a MAC address, or chosen a port, select this button and press  to display the results.

Learn: This displays how the switch recorded the particular MAC address. Dynamic means the switch recorded the address by sending out a query. Static means the address was entered manually through the Static MAC Addresses screen.

VLAN and GVRP Status

```
-----
                        VLAN and GVRP Status
-----

IEEE 802.1Q VLAN ID: <0018>
GARP status: Enabled                Number of IEEE 802.1Q VLANs: 106
Status: Dynamic (GVRP)
Creation time since switch power up: 00:00:00
Select switch: < Control  >
Current egress ports: 1, 2, 3, 4, 5, 6, 7, 8
Current untagged ports: 9, 10, 11, 12, 13, 14, 15

=====
Selects the next VLAN.
Esc = Previous screen  CTRL+R = Refresh  N = Next page  P = Previous Page
=====
```

LOCATION

- Main Menu
- Monitoring
- VLAN and GVRP Status

Description

This screen is available only if the switch is running tag-based (IEEE 802.1Q) VLANs. The screen shows information about one VLAN at a time. Press N or P to view status information for other tag-based VLANs on the switch.

IEEE 802.1Q VLAN ID: VLAN ID of the selected tag-based VLAN.

GARP status: Whether the VLAN can process GVRP requests.

Number of IEEE 802.1Q VLANs: Total number of tag-based VLANs (both static and dynamically created) currently configured on the switch.

Status: Whether the VLAN is permanent or dynamic. A permanent (static) tag-based VLAN is created and configured by the switch administrator. A dynamic VLAN is created by the switch in response to GVRP requests from GVRP-enabled network nodes.

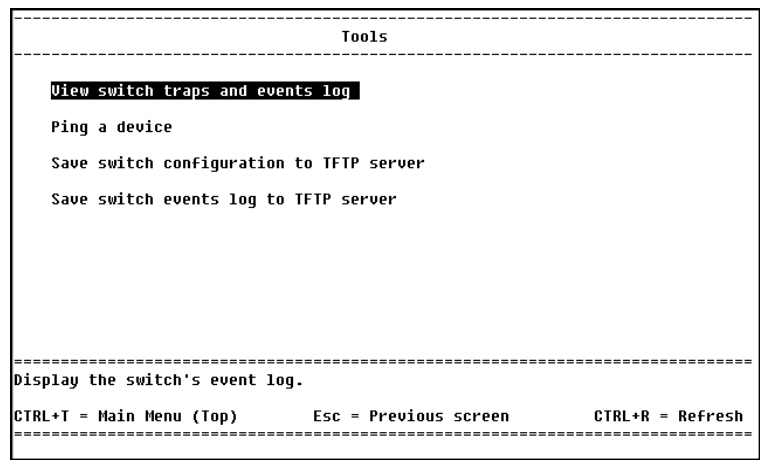
Creation time since switch power up: The amount of time since the switch was rebooted that the VLAN has been active.

Select switch: Press the Spacebar to select a switch.

Current egress ports: Lists all ports that belong to the specified tag-based VLAN.

Current untagged ports: Lists all ports that are configured to strip 802.1Q VLAN information from packets leaving the switch.

Tools



LOCATION

Main Menu
Tools

Description

- View switch traps and events log:** Events contained in the switch’s internal log.
- Ping a device:** Pings another device on the network to test connectivity.
- Save switch configuration to a TFTP server:** Backs up the switch’s current settings to a TFTP server.
- Save switch events log to a TFTP server:** Backs up the switch’s events log to a TFTP server.

Switch Event Log

Switch Event Log		
Seq.#	Time	Description
067	010d22h31m	STP status: Topology change.
066	009d12h18m	STP status: This switch became the new root of tree.
065	009d08h52m	Port 15 Link Up
064	008d01h35m	Port 16 is experiencing a broadcast storm!
063	007d00h13m	Port 12 is auto-partitioned.
062	007d04h12m	Operator logged out.
061	007d06h10m	Operation logged in with Administrator privilege.
060	007d10h09m	Successful login through telnet.
059	006d21h00m	Port 5 has lost link.
058	006d06h00m	Port 1 has changed speed to 100Mbps.
057	005d09h00m	Switch and Firmware 0S is fully operational.
056	005d02h00m	Power up. Express 530T Firmware 0S loaded.
- MORE - (12 of 154)		
Use the N, P, B, and E keys to view the log.		
N = Next Page P = Prev Page B = Log Begin E = Log End C = Clear Log		

LOCATION

Main Menu

Tools

View Switch Traps and...

Description

This screen allows you to view and navigate the switch's log. The log is similar to a trap and event receiver but it only captures traps/events generated by the switch itself. For example, the log includes events such as when a port is disabled, when an unauthorized user attempts to access a management interface, and when the switch reboots.

The log entries are listed chronologically from the last time the switch was rebooted. Use the following keys to navigate the log:

N = Next page

P = Previous page

B = Beginning of the log

E = End of the log

C = Clear the log

Ping a Device

Ping a Device

Target IP address: [999.999.999.999]
Repetitions: [999]
Timeout (sec): [999]
PING DEVICE (press any key to stop)

Result
=====

999.999.999 is alive, time = 999 ms.

=====

Enter the IP address of the device or station to ping.

CTRL+T = Main Menu (Top) Esc = Previous screen CTRL+R = Refresh

=====

LOCATION

Main Menu
Tools
Ping a Device

Description

Target IP address: Type the IP address of the device you want the switch to ping.

Repetitions: Type the number of times (1–255) you want the switch to send a ping to the specified device.

Timeout: Type the number of seconds (0–999) the switch waits before retrying a ping if it doesn’t receive a response from the first ping.

PING DEVICE: Select and press the Enter key to start pinging a device. To stop a ping, press any key on the keyboard.

Result: Displays the target device’s response to the ping.

Upload Configuration Image File

```

=====
                        Save Switch Configuration to TFTP Server
=====

Server IP address: [134.134.155.132]

Save Configuration to (filename):[                               ]

START

Result
=====

=====
IP address of the computer where the configuration is saved.

Ctrl+T=Main Screen (Top)      Esc = Previous screen      CTRL+R = Refresh
=====

```

LOCATION

Main Menu
Tools
Upload Configuration File

Description

This screen allows you to save an image of the switch's configuration to a file and upload it to a TFTP server.

Server IP address: The IP address of your TFTP server.

Save configuration to (filename): A file name and location to save the file on the server.

START: Select this button and press **Enter** to back up the switch settings.

NOTE

This feature creates an image of the switch configuration and saves it in binary format. This is not the same as a .cfg file, which is saved in ASCII text (see Appendix for information about configuration files).

Save Switch Events Log

Save Switch Events Log to TFTP Server

Server IP address: [124.123.123.80]

Save events logs to (filename):[]

START

Result

Type the IP address of the server to which you want to save the file.

Esc = Previous screen N = Next Page P = Prev Page CTRL+R = Refresh

LOCATION

- Main Menu
 - Tools
 - Save Switch Events Log...

Description

This screen allows you to save a list of the last 300 events to a file and upload it to a TFTP server.

Server IP address: Type the IP address of your TFTP server.

Save events log to (filename): Type a file name and location for where to save the file on the server.

START: Select this button and press Enter to save the events log.

A

Appendix: Technical Info

About Configuration Files

A configuration file is an ASCII text file that contains initialization information and configuration settings for the switch specified by the network administrator. The switch's configuration file (.CFG) can be up to 10KB in size and is stored on a central server where it is downloaded into the hub using TFTP.

You can use a text editor, such as Microsoft Windows* Notepad, to make changes to the configuration file. The switch interprets file lines beginning with the pound (#) sign as comments. It interprets all other lines as commands. When the switch initializes, it uses this file to configure parameters such as port speed, port security, and SNMP trap receivers.

Use of a standard configuration file can make managing multiple switches much simpler. Instead of requiring a network administrator to make changes to each manually, the switch uses the file to configure itself.

Sample Configuration File

The following is an example of a configuration file. For a more detailed explanation and additional keyword support, please visit the Intel Customer Support Web site at <http://support.intel.com/support/express/switches>.

```
##### Intel Express 530T Switch Configuration File #####
#
# Lines beginning with a "#" character are comment lines.

##### IP Address Configuration #####
#
# Ip_addr= <ipaddress>           IP address used by the switch
# Subnet_mask= <ipaddress>       Specify default gateway
# Default_gateway= <ipaddress>   Specify subnet mask
#
                                Ip_addr= 124.123.122.121
                                Subnet_mask= 255.255.255.0
                                Default_gateway= 124.123.122.254

##### Console and Configuration File Information #####
#
# Specify the code type of the image file
#
# Code_type=PROM      Image type is PROM code
# Code_type=RUNTIME   Image type is runtime firmware
# Code_type=CONFIG    Image type is saved configuration file

                                Code_type=PROM
#
# Image_file= <path>   Path and filename of runtime image or PROM image files

                                Image_file="e:\update\E530PROM.tftp"

##### Port Level Configuration #####
#
# Static_fdb_list={ (MAC address, port #)}      MAC address and port# of static entries
# Port_nway_enabled_list={port#, port#, . . }   Ports set to auto-negotiate
# Port_flow_ctrl_enabled_list= {port#, port#, . . } Ports that have flow control enabled
# Port_backpressure_enabled_list= {port#, port#, . . } Ports that have back pressure set
# Port_priority_list= { H (high), L (low), . . } Sets 802.1p priority queues
# Port_stp_enabled_list= {port#, port #, . . }  Ports that are enabled
# Port_disabled_list= {port#, port#, . . }       Ports that are disabled

                                Static_fdb_list={ (0080c8001121, 1) (0080c8001122, 2) (0080c8001123, 3) }
                                Port_nway_enabled_list={3,4,5,7}
                                Port_flow_ctrl_enabled_list = {3,4,5,7}
                                Port_backpressure_enabled_list = {16, 15, 14 }
                                Port_priority_list = { H,L,A,L,H,A,A,L,H }
                                Port_stp_enabled_list = {8,9,10,11, 20, 21,}
                                Port_disabled_list = { 20,21,22}
```



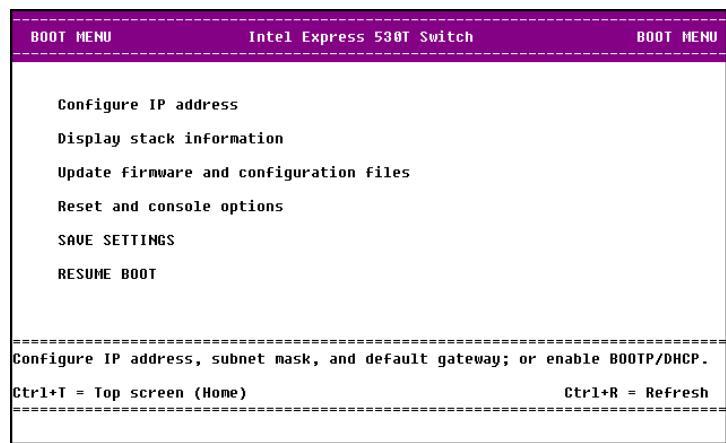
```
##### Link Aggregation #####
#
# linkaggr_list={(index "name", width of the aggregated group, "state"
#             index=from 1 to 4 (4=max number of aggregated groups possible)
#             name=name of the aggregated group
#             width=total port width of aggregated group
#             state="enable" or "disable" (default=disable)
#
#             linkaggr_list={(1 "Engineering Server", 2 "disable") (2 "Marketing Server", 3, "enable")
#             (3 "3rd Floor Switch", 2, "enable")}

##### Configure PVID for Untagged Ports #####
#
# pvid_list={(port#, PVIDvalue) (port#, PVIDvalue) ...}
#             port#=port attached to device that does not support tags
#             PVIDvalue=VID of port to which you want untagged traffic routed
#
#             pvid_list={(2, 100) (3, 100) (6, 15)}

##### Create 802.1Q VLAN on the Switch (Static Entries) #####
#
# 802_1q_static_list={(VID, "VLANstring", M/N U/T,...) (VID, "VLANstring", M/N U/T,...)}
#             M=member port (on ingress)
#             N=non member port (on ingress)
#             U=untagged device (on egress)
#             T=tagged device (on egress)
#             Either M or N can be specified for each port; not both
#             Either U or T can be specified for each port; not both
#
#             802_1q_static_list={(2, "VLAN2", MT, MU, MT, NT, MT, NU, NT, NU) (10, "VLAN10",
#             MU, NT, NT, MT, MU, NT, MU)}

##### GVRP (Dynamic VLAN Registration) #####
#
# gvrp_enabled={port#, port#, ...}
# gvrp_disabled={port#, port#, ...}
#             gvrp_enabled=VLAN dynamically registered with the switch
#             gvrp_disabled=VLAN not dynamically registered with the switch
#
#             gvrp_enabled={1, 3, 5, 7}
#             gvrp_disabled={2, 4, 6, 8}
```

BOOT Menu



Description

You usually don’t need to use the BOOT Menu. The BOOT Menu is available only by connecting to the switch’s serial port. It is used when the firmware fails to load.

To access the BOOT Menu, press **Ctrl** + **C** while the switch is starting up. The menu above displays. Most of the options available from the BOOT Menu are simplified versions of the normal runtime firmware; navigation is the same.

Configure IP address: Configures the switch’s IP address.

Display stack information: Configures identification and displays hardware information about all switches in the stack.

Update firmware and configuration files: Configures the switch’s internal software. Also used to specify the location of configuration files.

Reset and console options: Resets the switch to factory defaults to configure the port mode for the switch’s serial port. Also sets the console timeout.

SAVE SETTINGS: Saves the changes to the switch’s flash memory.

RESUME BOOT: Resumes the switch’s boot process and loading of the firmware.

List of Factory Defaults

- Software upgrade mode: Network
- Load configuration file: Disabled
- Console port data bits: 8
- IGMP snooping: Disabled
- Lock address table: Disabled
- System HOL-blocking state: Enabled
- System IGMP address: 192.0.2.1
- System default gateway: 0.0.0.0
- Port Nway state: Enabled (Auto-negotiate)
- Port backpressure state: Auto-negotiate
- Port HOL state: Enabled
- Ping repeat time: 1 time
- Port mirroring state: Disabled
- Port mirroring destination port: 2
- System bridge max age: 20 sec
- System bridge forward delay: 15 sec
- System aging time: 300 sec
- Per-port state: Enabled
- Read community string: Public
- Console user account: No username
- TFTP server address: 0.0.0.0
- Console baud rate: 9600
- Console port stop bit: 1
- System port partition state: Enabled
- MAC address Aging (sec): 300
- System console timeout: 15 minute
- System subnet mask: 255.255.255.0
- System BootP request: Enabled
- Port flow control state: Auto-negotiate IEEE 802.3x
- Port priority state: Use Frame Tag
- Ping IP address: 0.0.0.0
- Ping timeout: 5 sec
- Port mirroring source port: 1
- System spanning tree state: Disabled- IEEE 802.1d
- System bridge hello time: 2 sec
- System bridge priority: 32768
- Per-port spanning tree priority: 128
- Per-port spanning tree state: Enabled
- Write community string: Private
- Console user password: No password

Optional module default settings

- FX Module Port Speed: 100Mbps
- FX Module Flow Control: IEEE 802.3x
- SX/LX Module Port Speed: 1000Mbps
- SX Module Flow Control: IEEE 802.3x
- FX Module Port Duplex: Full Duplex
- FX Module Priority: Use Frame Tag
- SX/LX Module Port Duplex: Full-Duplex
- SX Module Priority: Use Frame Tag

Troubleshooting/FAQs

I booted the switch, and the status LED stays orange, is something wrong?

By default, the switch is in BootP mode, and the LED stays orange while the switch waits for an IP address from the BootP server. In order to proceed with the boot, either bypass the BootP phase (refer to the Quick Start guide for instructions), or manually assign an IP address.

If the switch doesn't receive an IP address from the BootP server within ten minutes, it will continue the boot process as normal.

How can I set the speed or duplex on individual ports?

Normally the switch handles all connections automatically but if you need to force speed or duplex, (for example, to accommodate older devices that don't support autonegotiation) use the Local Management or Web Device View.

When I set the 530T to autonegotiate with flow control enabled and try to connect to another device, there is no link. Why?

Check the settings of the other device and disable flow control. If you want to use flow control on the port, force the speed, duplex, and flow control settings so that they match.

I've connected the cable but the left LED (link) is off. Why?

- Remove the cable and plug it in again. Wait up to six seconds for a link.
- Make sure you're using the correct type of cable (straight-through-MDI or crossover-MDI-X) for the device you want to connect to. If you're using the wrong cable, the link LED will not come on.
- Make sure the device you've connected to a port is a 10Base-T or 100Base-TX device. The 530T switch doesn't support 100Base-T4 devices running at 100Mbps. However, it does support T4 devices running at 10Mbps.
- Check the speed and duplex settings on the PC's network adapter.
- The cable is defective.

The port's left LED (link) is on but I'm not seeing any activity when I try to ping a device on that port. Why?

- The port could be disabled through management. Go into the Local Management or Web Device view to enable the port and try pinging the device again.
- The port could be partitioned (auto-disabled). This condition is usually caused by a malfunctioning network adapter or an overloaded network segment. The switch will wait until it stops receiving collisions then clear the port automatically.

After I connect to Local Management I see a blank screen. Why?

- Make sure you are using a null modem cable (included).
- Check the settings in your terminal program. They should be set to 9600 baud, 8 data bits, No parity, 1 stop bit, and No flow control.
- Try pressing **Ctrl** + **Return** to force the screen to refresh.

I keep getting an intermittent loss of link. (or data is not being transmitted) Why?

- You may be using the wrong grade of cable. The wrong cable can cause erratic performance and you may eventually lose the connection between the port and the attached device.
- Check the duplex setting for the device connected to the port. You may have to use the Local Management or Web Device Manager to force the port to half or full duplex.
- A cable segment somewhere in your collision domain may be too long. Make sure none of your UTP cabling is longer than 100 meters.
- Check the Ethernet cable pairs. The TX pairs (pins 1 and 2) and the RX pairs (pins 3 and 6) should be twisted pairs. See diagram in Chapter 1.

I created a tag-based VLAN, and I have tag-capable LAN adapters in my PCs, but I can still communicate with devices outside the VLAN. Why?

Check to make sure that you have assigned a VID to the PC. If you don't assign a VID to the NIC in the PC it will behave as an untagged device. The default VID for untagged devices=1 so all untagged PCs will be a member of the DEFAULT_VLAN.

Can I stack 510, 520, or 550 switches with the 530T?

No. The only switch that can be stacked with the 530T is the 535T. You can stack up to three 535T switches with a 530T.

Locating MIB files

If you use a MIB browser, you can configure or view statistics for the switch. You can find these switch MIB files at the Intel Customer Support Web site at <http://support.intel.com/support/express/switches>.

- intel.mib
- int_gen.mib
- int_2530.mib
- int_pbrd.mib
- int_qprd.mib

When compiling the MIBs into an SNMP-compliant management application, compile the intel.mib first then compile the int_gen.mib, int_s530.mib, int_pbrd.mib, and int_qprb.mib files.

Regulatory Information

FCC Part 15 Compliance Statement

This product has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This product generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning this equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Change the direction of the radio or TV antenna.
- To the extent possible, relocate the radio, TV, or other receiver away from the product.
- Plug the product into a different electrical outlet so that the product and the receiver are on different branch circuits.

If these suggestions don't help, consult your dealer or an experienced radio/TV repair technician for more suggestions.

NOTE This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

CAUTION If you make any modification to the equipment not expressly approved by Intel, you could void your authority to operate the equipment.

Canada Compliance Statement (Industry Canada)

Cet appareil numérique respecte les limites bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministre Canadien des Communications. This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled: "Digital Apparatus," ICES-003 of the Canadian Department of Communications.

Manufacturer Declaration

This certifies that the Intel® Express 530T Switch complies with the EU Directive 89/336/EEC, using the EMC standards EN55022 (Class A) and EN55024. This product also meets or exceeds EN 60950 (safety) requirements. These products have been tested and verified to meet CISPR 22 Class A requirements.

Australia Statement



Taiwan Class A EMI Statement

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

VCCI Statement

Class A ITE

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Warnings

WARNING

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Internal access to Intel® Express 530T Switch intended only for qualified service personnel. Do not remove any covers.

WARNING

The system is designed to operate in a typical office environment. Choose a site that is:

- Clean and free of airborne particles (other than normal room dust).
- Well ventilated and away from sources of heat including direct sunlight.
- Away from sources of vibration or physical shock.
- Isolated from strong electromagnetic fields produced by electrical devices.
- In regions that are susceptible to electrical storms, we recommend you plug your system into a surge suppressor and disconnect telecommunication lines to your modem during an electrical storm.
- Provided with a properly grounded wall outlet.

Do not attempt to modify or use the supplied AC power cord if it is not the exact type required.

Ensure that the system is disconnected from its power source and from all telecommunications links, networks, or modems lines whenever the chassis cover is to be removed. Do not operate the system with the cover removed.

AVERTISSEMENT

Le système a été conçu pour fonctionner dans un cadre de travail normal. L'emplacement choisi doit être:

- Propre et dépourvu de poussière en suspension (sauf la poussière normale).
- Bien aéré et loin des sources de chaleur, y compris du soleil direct.
- A l'abri des chocs et des sources de vibrations.
- Isolé de forts champs magnétiques générés par des appareils électriques.
- Dans les régions sujettes aux orages magnétiques il est recommandé de brancher votre système à un supresseur de surtension, et de débrancher toutes les lignes de télécommunications de votre modem durant un orage.
- Muni d'une prise murale correctement mise à la terre.

Ne pas utiliser ni modifier le câble d'alimentation C. A. fourni, s'il ne correspond pas exactement au type requis.

Assurez vous que le système soit débranché de son alimentation ainsi que de toutes les liaisons de télécommunication, des réseaux, et des lignes de modem avant d'enlever le capot. Ne pas utiliser le système quand le capot est enlevé.

WARNUNG

Das System wurde für den Betrieb in einer normalen Büroumgebung entwickelt. Der Standort sollte:

- sauber und staubfrei sein (Hausstaub ausgenommen);
- gut gelüftet und keinen Heizquellen ausgesetzt sein (einschließlich direkter Sonneneinstrahlung);
- keinen Erschütterungen ausgesetzt sein;
- keine starken, von elektrischen Geräten erzeugten elektromagnetischen Felder aufweisen;
- in Regionen, in denen elektrische Stürme auftreten, mit einem Überspannungsschutzgerät verbunden sein; während eines elektrischen Sturms sollte keine Verbindung der Telekommunikationsleitungen mit dem Modem bestehen;
- mit einer geerdeten Wechselstromsteckdose ausgerüstet sein.

Versuchen Sie nicht, das mitgelieferte Netzkabel zu ändern oder zu verwenden, wenn es sich nicht um genau den erforderlichen Typ handelt.

Das System darf weder an eine Stromquelle angeschlossen sein noch eine Verbindung mit einer Telekommunikationseinrichtung, einem Netzwerk oder einer Modem-Leitung haben, wenn die Gehäuseabdeckung entfernt wird. Nehmen Sie das System nicht ohne die Abdeckung in Betrieb.

AVVERTENZA

Il sistema è progettato per funzionare in un ambiente di lavoro tipico. Scegliere una postazione che sia:

- Pulita e libera da particelle in sospensione (a parte la normale polvere presente nell'ambiente).
- Ben ventilata e lontana da fonti di calore, compresa la luce solare diretta.
- Al riparo da urti e lontana da fonti di vibrazione.
- Isolata dai forti campi magnetici prodotti da dispositivi elettrici.
- In aree soggette a temporali, è consigliabile collegare il sistema ad un limitatore di corrente. In caso di temporali, scollegare le linee di comunicazione dal modem.
- Dotata di una presa a muro correttamente installata.

Non modificare o utilizzare il cavo di alimentazione in c. a. fornito dal produttore, se non corrisponde esattamente al tipo richiesto.

Prima di rimuovere il coperchio del telaio, assicurarsi che il sistema sia scollegato dall'alimentazione, da tutti i collegamenti di comunicazione, reti o linee di modem. Non avviare il sistema senza aver prima messo a posto il coperchio.

ADVERTENCIAS

El sistema está diseñado para funcionar en un entorno de trabajo normal. Escoja un lugar:

- Limpio y libre de partículas en suspensión (salvo el polvo normal)
- Bien ventilado y alejado de fuentes de calor, incluida la luz solar directa.
- Alejado de fuentes de vibración.
- Aislado de campos electromagnéticos fuertes producidos por dispositivos eléctricos.
- En regiones con frecuentes tormentas eléctricas, se recomienda conectar su sistema a un eliminador de sobrevoltage y desconectar el módem de las líneas de telecomunicación durante las tormentas.
- Previsto de una toma de tierra correctamente instalada.

No intente modificar ni usar el cable de alimentación de corriente alterna, si no se corresponde exactamente con el tipo requerido.

Asegúrese de que cada vez que se quite la cubierta del chasis, el sistema haya sido desconectado de la red de alimentación y de todos los enlaces de telecomunicaciones, de red y de líneas de módem. No ponga en funcionamiento el sistema mientras la cubierta esté quitada.

Wichtige Sicherheitshinweise

- 1** Bitte lesen Sie sich diese Hinweise sorgfältig durch.
- 2** Heben Sie diese Anleitung für den spätem Gebrauch auf.
- 3** Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie keine Flüssig- oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
- 4** Um eine Beschädigung des Gerätes zu vermeiden sollten Sie nur Zubehörteile verwenden, die vom Hersteller zugelassen sind.
- 5** Das Gerät ist vor Feuchtigkeit zu schützen.
- 6** Bei der Aufstellung des Gerätes ist auf sichern Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen. Verwenden Sie nur sichere Standorte und beachten Sie die Aufstellhinweise des Herstellers.
- 7** Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor Überhitzung schützt. Sorgen Sie dafür, daß diese Öffnungen nicht abgedeckt werden.
- 8** Beachten Sie beim Anschluß an das Stromnetz die Anschlußwerte.
- 9** Die Netzanschlußsteckdose muß aus Gründen der elektrischen Sicherheit einen Schutzleiterkontakt haben.
- 10** Verlegen Sie die Netzanschlußleitung so, daß niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
- 11** Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
- 12** Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
- 13** Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. Elektrischen Schlag auslösen.
- 14** Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von autorisiertem Servicepersonal geöffnet werden.
- 15** Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einerqualifizierten Servicestelle zu überprüfen:
 - a** Netzkabel oder Netzstecker sind beschädigt.
 - b** Flüssigkeit ist in das Gerät eingedrungen.
 - c** Das Gerät war Feuchtigkeit ausgesetzt.
 - d** Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
 - e** Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
 - f** Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
- 16** Bei Reparaturen dürfen nur Originalersatzteile bzw. den Originalteilen entsprechende Teile verwendet werden. Der Einsatz von ungeeigneten Ersatzteilen kann eine weitere Beschädigung hervorrufen.
- 17** Wenden Sie sich mit allen Fragen die Service und Reparatur betreffen an Ihren Servicepartner. Somit stellen Sie die Betriebssicherheit des Gerätes sicher.
- 18** Zum Netzanschluß dieses Gerätes ist eine geprüfte Leitung zu verwenden, Für einen Nennstrom bis 6A und einem Gerätegewicht größer 3kg ist eine Leitung nicht leichter als H05VV-F, 3G, 0.75mm² einzusetzen.

Limited Hardware Warranty

Intel warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship for three (3) years following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within thirty (30) days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

INTEL RESERVES THE RIGHT TO FILL YOUR ORDER WITH A PRODUCT CONTAINING NEW OR REMANUFACTURED COMPONENTS. THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF NONINFRINGEMENT OF INTELLECTUAL PROPERTY, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION, SAMPLE OR OTHERWISE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number either to the company from whom you purchased it or to Intel (North America only). If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either new or remanufactured product or parts, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original three (3) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA)

Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling:

- **North America only:** (916) 377-7000
- **Other locations:** Return the product to the place of purchase.

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

LIMITATION OF LIABILITY AND REMEDIES

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitations or exclusions may not apply to you.

Critical Control Applications: Intel specifically disclaims liability for use of the hardware product in critical control applications (including, for example only, safety or health care control systems, nuclear energy control systems, or air or ground traffic control systems) by Licensee or Sublicensees, and such use is entirely at the user's risk. Licensee agrees to defend, indemnify, and hold Intel harmless from and against any and all claims arising out of use of the hardware product in such applications by Licensee or Sublicensees.

Software: Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

Limited Hardware Warranty (Europe only)

Intel warrants to the original owner that the hardware product delivered in this package will be free from defects in material and workmanship for three (3) years following the latter of: (i) the date of purchase only if you register by returning the registration card as indicated thereon with proof of purchase; or (ii) the date of manufacture; or (iii) the registration date if by electronic means provided such registration occurs within thirty (30) days from purchase. This warranty does not cover the product if it is damaged in the process of being installed. Intel recommends that you have the company from whom you purchased this product install the product.

INTEL RESERVES THE RIGHT TO FILL YOUR ORDER WITH A PRODUCT CONTAINING NEW OR REMANUFACTURED COMPONENTS. THE ABOVE WARRANTY IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF NONINFRINGEMENT OF INTELLECTUAL PROPERTY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION, SAMPLE OR OTHERWISE.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing. If the product is found to be otherwise defective, Intel, at its option, will replace or repair the product at no charge except as set forth below, provided that you deliver the product along with a return material authorization (RMA) number either to (a) the company from whom you purchased it or (b) to Intel, North America only (if purchased in Europe you must deliver the product to "(a)"). If you ship the product, you must assume the risk of damage or loss in transit. You must use the original container (or the equivalent) and pay the shipping charge. Intel may replace or repair the product with either new or remanufactured product or parts, and the returned product becomes Intel's property. Intel warrants the repaired or replaced product to be free from defects in material and workmanship for a period of the greater of: (i) ninety (90) days from the return shipping date; or (ii) the period of time remaining on the original three (3) year warranty.

This warranty gives you specific legal rights and you may have other rights which vary from state to state. All parts or components contained in this product are covered by Intel's limited warranty for this product; the product may contain fully tested, recycled parts, warranted as if new. For warranty information call one of the numbers below.

Returning a Defective Product (RMA)

Before returning any product, contact an Intel Customer Support Group and obtain an RMA number by calling the non-toll free numbers below:

Country	Number	Language
France	+33 (0) 1 41 91 85 29	French
Germany	+49 (0) 69 9509 6099	German
Italy	+39 (0) 2 696 33276	Italian
UK	+44 (0) 870 607 2439	English

If the Customer Support Group verifies that the product is defective, they will have the Return Material Authorization Department issue you an RMA number to place on the outer package of the product. Intel cannot accept any product without an RMA number on the package.

LIMITATION OF LIABILITY AND REMEDIES

INTEL SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER INTEL HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, INFRINGEMENT OF INTELLECTUAL PROPERTY, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, INTEL'S TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. INTEL NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

Critical Control Applications: Intel specifically disclaims liability for use of the hardware product in critical control applications (including, for example only, safety or health care control systems, nuclear energy control systems, or air or ground traffic control systems) by Licensee or Sublicensees, and such use is entirely at the user's risk. Licensee agrees to defend, indemnify, and hold Intel harmless from and against any and all claims arising out of use of the hardware product in such applications by Licensee or Sublicensees.

Software: Software provided with the hardware product is not covered under the hardware warranty described above. See the applicable software license agreement which shipped with the hardware product for details on any software warranty.

This limited hardware warranty shall be governed by and construed in accordance with the laws of England and Wales. The courts of England shall have exclusive jurisdiction regarding any claim brought under this warranty.

Limitation de garantie du materiel (Europe)

Intel garantit au propriétaire original que le produit matériel livré dans le présent coffret est exempt de défaut matériel ou de fabrication pour une période de trois (3) ans à compter de la plus récente des dates suivantes : (i) la date d'achat uniquement si vous vous êtes inscrit en renvoyant la carte d'inscription de la façon indiquée, avec une preuve d'achat ; (ii) la date de fabrication ou (iii) la date d'inscription électronique à condition qu'elle ait lieu dans les 30 jours suivant l'achat. La présente garantie sera nulle si le produit matériel est endommagé lors de son installation. Intel recommande de faire installer le produit matériel par la société auprès de laquelle il a été acheté.

INTEL SE RESERVE LE DROIT DE VOUS LIVRER UN PRODUIT CONTENANT DES COMPOSANTS NOUVEAUX OU REPARÉS. CETTE GARANTIE REMPLACE TOUTES LES AUTRES GARANTIES, EXPRESSES, TACITES OU LEGALES, Y COMPRIS, MAIS SANS QUE CETTE ENUMERATION SOIT LIMITATIVE, LES GARANTIES CONCERNANT LE NON RESPECT DE LA PROPRIETE INTELLECTUELLE, LA QUALITE SATISFAISANTE, L'ADEQUATION POUR UN USAGE PARTICULIER, OU TOUTE AUTRE GARANTIE ISSUE DE TOUT AUTRE PROPOSITION, SPECIFICATION, ECHANTILLON OU AUTRE.

La présente garantie ne couvre pas le remplacement de produits matériels endommagés par abus, accident, mauvaise utilisation, négligence, altération, réparation, catastrophe, installation ou tests incorrects. Si le produit matériel s'avère défectueux pour une autre raison, Intel décidera de le remplacer ou de le réparer gratuitement, à l'exception des cas énumérés ci-après, à condition que le produit soit renvoyé avec un numéro d'autorisation de retour du matériel (ARM) à (a) la société auprès de laquelle il a été acheté ou (b) à Intel, en Amérique du Nord seulement (si l'achat a eu lieu en Europe vous devez le renvoyer à "(a)"). Si vous expédiez le produit matériel, vous devez assumer le risque de dégâts ou de perte pendant le transport. Vous devez utiliser le coffret original (ou l'équivalent) et payer les frais de transport. Intel peut réparer le produit matériel ou le remplacer par un produit neuf ou remis à neuf, le produit renvoyé devenant la propriété d'Intel. Intel garantit que le produit matériel réparé ou de remplacement est exempt de défaut matériel ou de fabrication pendant la plus longue des périodes suivantes: (i) quatre-vingt-dix (90) jours à compter de la date de retour; ou (ii) la période encore couverte par la garantie originale de trois (3) ans.

La présente garantie vous accorde des droits juridiques spécifiques et vous pouvez également disposer d'autres droits variant d'un Etat à l'autre. Tous les composants ou pièces du produit matériel sont couverts par la garantie limitée d'Intel relative à ce dernier ; il peut contenir des pièces recyclées, entièrement testées et garanties comme neuves. Pour plus d'informations sur la garantie, appelez l'un des numéros énumérés ci-après.

Retour d'un produit défectueux (ARM)

Avant de retourner un produit matériel, contactez le service d'assistance à la clientèle Intel pour obtenir un numéro ARM.

Pays	Numéro	Langue
France	+33 (0) 1 41 91 85 29	Français
Allemagne	+49 (0) 69 9509 6099	Allemand
Italie	+39 (0) 2 696 33276	Italien
R.U.	+44 (0) 870 607 2439	Anglais

Si le service d'assistance confirme que le produit est défectueux, il demandera au Département d'autorisation de retour de matériel de vous attribuer un numéro ARM à indiquer sur l'emballage externe. Intel ne peut accepter aucun produit sans numéro ARM.

LIMITATION DE RESPONSABILITE ET DE RECOURS

INTEL DECLINE TOUTE RESPONSABILITE RELATIVE A DES DOMMAGES INDIRECTS OU SPECULATIFS (Y COMPRIS, SANS LIMITATION DES ELEMENTS CI-DESSUS, LES DOMMAGES CONSECUTIFS, ACCIDENTELS ET SPECIAUX) DECOULANT DE L'UTILISATION OU DE L'INCAPACITE D'UTILISER CE PRODUIT, DUS A UN CONTRAT, UNE NEGLIGENCE, UN TORT OU COUVERTS PAR TOUTE GARANTIE, MEME SI LA POSSIBILITE D'UN TEL DOMMAGE A DEJA ETE PORTEE A LA CONNAISSANCE D'INTEL, Y COMPRIS, MAIS SANS QUE CETTE ENUMERATION SOIT LIMITATIVE, UNE PRIVATION DE JOUISSANCE, UN NON RESPECT DE LA PROPRIETE INTELLECTUELLE, UNE INTERRUPTION DES ACTIVITES ET UN MANQUE A GAGNER . NONOBTANT LA DECLARATION QUI PRECEDE, LA RESPONSABILITE GLOBALE DE INTEL CONCERNANT TOUS LES LITIGES RELATIFS AU PRESENT ACCORD NE SERA PAS SUPERIEURE AU PRIX PAYE POUR LE PRODUIT. CES LIMITATIONS DE RESPONSABILITE POTENTIELLE ONT CONSTITUE UN FACTEUR DETERMINANT LORS DE LA FIXATION DU PRIX DU PRODUIT. INTEL N'ASSUME AUCUNE AUTRE RESPONSABILITE ET N'AUTORISE QUICONQUE A LE FAIRE EN SON NOM.

Applications de contrôle critique: Intel décline toute responsabilité en cas d'utilisation du produit matériel dans le cadre d'applications de contrôle critique (y compris et pour ne citer que des exemples, les systèmes de contrôle de sécurité ou de services médicaux, les systèmes de contrôle d'énergie nucléaire, ou de trafic terrestre ou aérien) par le licencié ou le sous-licencié, l'utilisateur encourt entièrement les risques d'une telle utilisation. Le titulaire de la licence accepte de défendre, d'indemniser et de garantir Intel de toute réclamation survenant par suite de l'utilisation du produit matériel dans de telles applications par le licencié ou le sous-licencié.

Logiciel: Le logiciel fourni avec le produit matériel n'est pas couvert par la garantie du matériel décrite ci-dessus. Consultez l'accord de licence du logiciel qui accompagne le produit matériel pour obtenir des détails sur la garantie du logiciel.

La garantie limitée du matériel est régie et interprétée par les lois en vigueur en Angleterre et au Pays de Galles. Les tribunaux anglais jouissent d'une juridiction exclusive en matière de litige concernant cette garantie.

Garanzia limitata sull'hardware (valida solo in Europa)

Intel garantisce al proprietario originale che il prodotto hardware incluso in questo pacchetto è privo di difetti in materiale e in lavorazione per un periodo di tre (3) anni a partire dall'ultima data tra: (i) la data di acquisto, solo nel caso in cui l'utente effettua la registrazione tramite la scheda di registrazione, come indicato, accompagnata dalla prova di acquisto; oppure (ii) la data di fabbricazione; oppure (iii) la data di registrazione, se effettuata per via elettronica, a condizione che tale registrazione avvenga entro trenta (30) giorni dall'acquisto. Questa garanzia non copre il prodotto nel caso questo fosse danneggiato durante l'installazione. Intel raccomanda di fare installare il prodotto dall'azienda da cui il prodotto è stato acquistato.

INTEL SI RISERVA IL DIRITTO DI ONORARE L'ORDINAZIONE CON UN PRODOTTO CONTENENTE PARTI NUOVE O RIFABBRICATO. LA GARANZIA QUI SOPRA SOSTITUISCE QUALSIASI ALTRA GARANZIA, SIA QUELLA ESPLICITA, IMPLICITA O STATUTORIA, INCLUSO, MA NON LIMITATO A, QUALSIASI GARANZIA DI NON VIOLAZIONE DI PROPRIETÀ INTELLETTUALE, QUALITÀ SODDISFACENTE, IDONEITÀ A QUALSIASI SCOPO PARTICOLARE O QUALSIASI GARANZIA DERIVANTE DA PROPOSTA, SPECIFICAZIONI, CAMPIONI O ALTRO.

Questa garanzia non include la sostituzione di prodotti danneggiati a causa di abuso, incidente, uso inappropriato, negligenza, alterazione, riparazione, disastro, installazione o controllo inadeguati. Se il prodotto viene considerato difettoso per altri motivi, Intel, a sua discrezione, sostituirà o riparerà il prodotto, a proprie spese, eccetto nei casi qui sotto menzionati, a condizione che il prodotto venga consegnato congiuntamente al numero di autorizzazione per la restituzione del materiale (RMA, Return Material Authorization) (a) all'azienda da cui si è acquistato il prodotto, oppure (b) a Intel, solo quando in Nord America (se il prodotto è stato acquistato in Europa, sarà necessario consegnare il prodotto seguendo le modalità indicate in "(a)"). Se il prodotto viene inviato, il mittente si assume la responsabilità in caso di danni o di perdita durante il tragitto. È necessario utilizzare l'imballaggio originale del prodotto (o un suo equivalente) e pagare le spese di spedizione. Intel sostituirà o riparerà il prodotto (o la parte) con uno nuovo o uno rifabbricato, e il prodotto restituito diventerà proprietà di Intel. Intel garantisce che il prodotto riparato o sostituito sarà privo di difetti in materiale e in lavorazione per un periodo comunque non superiore: (i) a novanta (90) giorni dalla data di spedizione all'utente; oppure (ii) al periodo rimanente nella garanzia originale di tre (3) anni.

Questa garanzia dà all'utente diritti legali specifici; potrebbero esistere altri diritti, variabili da stato a stato. Tutte le parti e i componenti contenuti in questo prodotto sono coperti dalla garanzia limitata di Intel relativa a questo prodotto; il prodotto potrebbe contenere parti riciclate, completamente collaudate e garantite come nuove. Per maggiori informazioni sulla garanzia, chiamare uno dei numeri indicati qui sotto.

Restituzione di prodotti difettosi (RMA)

Prima di restituire un prodotto, contattare l'assistenza tecnica di Intel e richiedere un numero RMA; i numeri verdi sono qui sotto elencati:

Paese	Numero	Lingua
Francia	+33 (0) 1 41 91 85 29	Francese
Germania	+49 (0) 69 9509 6099	Tedesco
Italia	+39 (0) 2 696 33276	Italiano
Regno Unito	+44 (0) 870 607 2439	Inglese

Se il gruppo di supporto alla clientela determina che il prodotto è difettoso, richiederà l'emissione di un numero di autorizzazione per la restituzione del materiale (RMA) da porre all'esterno dell'imballaggio del prodotto. Intel non accetterà prodotti sprovvisti di tale numero visibile sull'imballaggio.

LIMITAZIONI DI RESPONSABILITÀ E RIMEDI

INTEL NON POTRÀ ESSERE CONSIDERATA RESPONSABILE DI ALCUN DANNO, DIRETTO O SPECULATIVO (INCLUSI, SENZA LIMITAZIONI COME INDICATO IN PRECEDENZA, I DANNI CONSEGUENZIALI, INCIDENTALI E SPECIALI) DERIVANTI DALL'USO O DALLA IMPOSSIBILITÀ DI UTILIZZARE QUESTO PRODOTTO, PER MOTIVI NON CONTEMPLATI NEL CONTRATTO, O DOVUTI A NEGLIGENZA, TORTO O SOTTO QUALSIASI GARANZIA, INDIPENDENTEMENTE DAL FATTO CHE INTEL SIA A CONOSCENZA O MENO DELLA POSSIBILITÀ DI TALI DANNI, INCLUSI, MA NON LIMITATI ALLA PERDITA D'USO, VIOLAZIONE DI PROPRIETÀ INTELLETTUALE, INTERRUZIONI D'AFFARI E PERDITA DI PROFITTI, NONOSTANTE QUANTO DETTO IN PRECEDENZA, LA RESPONSABILITÀ TOTALE DI INTEL NEI CONFRONTI DEI RECLAMI, SECONDO QUESTO ACCORDO, NON ECCEDERÀ IL PREZZO PAGATO PER IL PRODOTTO. QUESTE LIMITAZIONI SULLE RESPONSABILITÀ POTENZIALI SONO STATE FATTORE DECISIVO NELLA DETERMINAZIONE DEL PREZZO DEL PRODOTTO. INTEL NON ASSUME, NÉ AUTORIZZA ALCUNO AD ASSUMERE PER SÉ, NESSUN'ALTRA RESPONSABILITÀ.

Applicazioni di controllo di situazioni critiche: Intel disconosce specificatamente la responsabilità nel caso di uso dell'hardware in applicazioni di controllo di situazioni critiche (inclusi, al solo scopo di esempio, sistemi di controllo della sicurezza o della salute, dell'energia nucleare, o sistemi di controllo aereo o terrestre) da parte dei licenziatari o dei sottollicenziatari, e tale uso fa parte completamente del rischio intrapreso dall'utente. Il licenziatario è d'accordo nel difendere, indennizzare e liberare Intel da ogni reclamo risultante dall'uso del prodotto hardware in tale applicazioni da parte del licenziatario o del sottollicenziatario.

Software: il software incluso al prodotto hardware non è coperto dalla garanzia dell'hardware sopra descritta. Per maggiori dettagli sulla garanzia del software, vedere l'accordo di licenza relativo al software, inviato assieme al prodotto hardware.

Questa garanzia limitata dell'hardware è governata da, ed è conforme a, le leggi di Inghilterra e Galles. Il tribunale di Inghilterra avrà la completa giurisdizione su qualsiasi reclamo presentato sotto questa garanzia.

Beschränkte Hardwaregarantie (Nur für Europa)

Intel garantiert dem ursprünglichen Eigentümer, daß die in diesem Paket enthaltene Hardware keine Material- oder Herstellungsfehler aufweist. Diese Garantie gilt für drei (3) Jahre (a) nach dem Kaufdatum, wenn die ausgefüllte Registrierungskarte entsprechend den darauf enthaltenen Angaben zusammen mit einem Kaufnachweis eingesendet wurde; oder (b) nach dem Herstellungsdatum; oder (c) nach dem Registrierungsdatum, wenn die Registrierung innerhalb von 30 Tagen auf elektronischem Weg durchgeführt wird. Diese Garantie entfällt, wenn die Hardware bei der Installation beschädigt wird. Intel empfiehlt, die Installation durch den Verkäufer der Hardware durchführen zu lassen.

INTEL BEHÄLT SICH DAS RECHT VOR, IHREN AUFTRAG MIT EINEM PRODUKT ZU ERFÜLLEN, DAS NEUE ODER ERNEUERTE KOMPONENTEN ENTHÄLT. OBIGE GARANTIE GILT ANSTELLE ALLER ANDEREN AUSDRÜCKLICHEN, STILLSCHWEIGENDEN ODER GESETZLICH FESTGELEGTEN GARANTIEEN. AUSGESCHLOSSEN SIND DAMIT AUCH UNTER ANDEREM ALLE GARANTIEEN FÜR DIE VERKEHRSFÄHIGKEIT, DIE VERLETZUNG DER RECHTE VON DRITTEN, DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER GARANTIEEN, DIE IM ZUSAMMENHANG MIT EINEM ANGEBOT, EINER SPEZIFIKATION ODER EINEM MUSTER GEGEBEN WURDEN.

Diese Garantie schließt den Hardware-Ersatz bei Beschädigung aufgrund von Mutwilligkeit, Unfall, falscher Verwendung, Fahrlässigkeit, Umänderung, Reparatur, Katastrophen, falscher Installation oder unvorschriftsmäßigem Testen aus. Wenn das Hardwareprodukt aus anderen Gründen beschädigt ist, liegt die Entscheidung bei Intel, ob die Hardware mit Ausnahme der im folgenden beschriebenen Einschränkungen kostenlos ersetzt oder repariert wird. Hierzu müssen Sie das Produkt zusammen mit einer Rückgabenummer (RMA-Nummer, siehe unten) entweder (a) an den Verkäufer des Produkts oder (b) an Intel zurücksenden (bei Kauf in Europa muß das Produkt an "(a)" geliefert werden). Das Risiko des Verlusts oder der Beschädigung während des Transports liegt bei Ihnen als Käufer. Sie müssen zum Versenden die Originalverpackung (oder einen gleichwertigen Ersatz) verwenden und die Versandkosten übernehmen. Intel ersetzt die Hardware entweder durch ein neues oder ein neuwertiges Produkt. Das zurückgegebene Hardwareprodukt wird Eigentum von Intel. Intel garantiert, daß das reparierte oder ersetzte Hardwareprodukt für einen Zeitraum von: (i) neunzig (90) Tagen ab Rückgabedatum oder (ii) für die verbleibende Zeit der ursprünglichen Garantie von drei (3) Jahren frei von Material- und Herstellungsfehlern ist. Dabei gilt jeweils der längere Zeitraum.

Mit dieser Garantie erhalten Sie bestimmte Rechte, die je nach Staat durch weitere Rechte ergänzt werden können. Alle Teile oder Komponenten dieses Hardwareprodukts werden durch die beschränkte Hardwaregarantie von Intel abgedeckt. Das Hardwareprodukt kann vollständig getestete, wiederverwendete Teile enthalten, die derselben Garantie wie neue Produkte unterliegen. Informationen zur Garantie erhalten Sie unter einer der Intel Kundendienstnummern, die am Ende dieses Handbuchs zu finden sind.

Rückgabe eines beschädigten Produkts (RMA)

Bevor Sie ein Hardwareprodukt zurücksenden, sollten Sie sich vom Intel Kundendienst eine sogenannte RMA-Nummer zuweisen lassen, indem Sie eine der folgenden gebührenpflichtigen Telefonnummern anrufen:

Land	Telefon	Sprache
Frankreich	+33 (0) 1 41 91 85 29	Französisch
Deutschland	+49 (0) 69 9509 6099	Deutsch
Italien	+39 (0) 2 696 33276	Italienisch
GB	+44 (0) 870 607 2439	Englisch

Nachdem die Beschädigung vom Kundendienst bestätigt worden ist, wird von der zuständigen Abteilung eine Rückgabenummer (RMA-Nummer) ausgegeben, die auf der äußeren Verpackung der Hardware angebracht werden muß. Intel akzeptiert kein Produkt ohne RMA-Nummer auf der Verpackung.

Haftungsbeschränkung und Rechtsmittel

INTEL HAFTET NICHT FÜR INDIREKTE ODER SPEKULATIVE SCHÄDEN (EINSCHLIESSLICH ALLER FOLGESCHÄDEN SOWIE ALLER ZUFÄLLIGEN UND BESONDEREN SCHÄDEN), DIE DURCH DIE VERWENDUNG ODER NICHTVERWENDBARKEIT DIESES PRODUKTS ENTSTEHEN, SEI DIES IM ZUSAMMENHANG MIT EINER VERTRAGLICHEN VERPFLICHTUNG, AUFGRUND VON FAHRLÄSSIGKEIT, DURCH UNERLAUBTE HANDLUNGEN ODER IM RAHMEN EINER GARANTIE. DIES GILT AUCH FÜR FÄLLE, IN DENEN INTEL ÜBER DIE MÖGLICHKEIT SOLCHER SCHÄDEN, DIE SICH UNTER ANDEREM DURCH NUTZUNGS-AUSFÄLLE, BETRIEBSUNTERBRECHUNGEN UND GEWINNVERLUSTE ERGEBEN KÖNNEN, IN KENNTNIS GESETZT WURDE.

UNGEACHTET DER GEWÄHRTEN GARANTIE ÜBERSTEIGT DIE HAFTUNG VON INTEL IM RAHMEN DIESER VEREINBARUNG IN KEINEM FALL DEN KAUFPREIS DES HARDWAREPRODUKTS. DIESE HAFTUNGSBESCHRÄNKUNG IST EIN WESENTLICHER FAKTOR BEI DER FESTLEGUNG DES PREISES FÜR DAS HARDWAREPRODUKT. INTEL ÜBERNIMMT KEINE WEITERE HAFTUNG UND ERTEILT DRITTEN KEINERLEI BEFUGNIS, FÜR INTEL EINE WEITERE HAFTUNG ZU ÜBERNEHMEN.

Steuer- und Überwachungsanwendung von hoher Wichtigkeit: Intel schließt insbesondere die Haftung bei der Verwendung des Hardwareprodukts mit Steueranwendungen von hoher Wichtigkeit (z.B. Sicherheits- und Krankenversicherungssysteme, Steuersysteme für Nuklearanlagen sowie Verkehrsüberwachungssysteme für Boden- und Luftverkehr) durch den Lizenznehmer oder Unterlizenznehmer ab, und eine derartige Verwendung liegt ausschließlich in der Verantwortung des Benutzers. Der Lizenznehmer erklärt sich bereit, Intel zu verteidigen und schadlos zu halten bezüglich aller Klagen, die aus der Verwendung eines Hardwareprodukts für solche Zwecke vom Lizenznehmer oder Unterlizenznehmern erhoben werden.

Software: Die mit diesem Hardwareprodukt gelieferte Software wird von der oben beschriebenen Hardwaregarantie nicht abgedeckt. Bitte lesen Sie die entsprechende Softwarelizenzvereinbarung, die mit dem Hardwareprodukt geliefert wurde, um genaue Informationen zur Softwaregarantie zu erhalten.

Diese eingeschränkte Hardwaregarantie unterliegt den Gesetzen von England und Wales. Die englischen Gerichte sind Gerichtsstand für alle Klagen, die im Rahmen der Garantie erhoben werden.

Garantía limitada de hardware (solo para Europa)

Intel garantiza al propietario original que el producto de hardware entregado en este paquete no tendrá defectos de materiales ni fabricación durante tres (3) años contados a partir de la fecha que resulte más reciente de entre las opciones siguientes: (i) la fecha de compra, sólo si devuelve la tarjeta de registro con prueba de compra de la forma indicada al respecto para registrarse; o bien (ii) la fecha de fabricación; o (iii) la fecha de registro, si éste se ha producido por medios electrónicos y dentro de los treinta (30) días siguientes a la compra. Esta garantía no cubre los daños sufridos por el producto durante el proceso de instalación. Intel recomienda que sea la empresa a la que adquirió el producto la que se encargue de su instalación.

INTEL SE RESERVA EL DERECHO DE CUMPLIMENTAR EL PEDIDO CON UN PRODUCTO QUE CONTENGA COMPONENTES NUEVOS O REFRABRICADOS. LA GARANTÍA ANTERIOR PREVALECE SOBRE CUALQUIER OTRA GARANTÍA, YA SEA EXPLÍCITA, IMPLÍCITA O REGLAMENTARIA, INCLUIDAS, SIN LIMITACIÓN, CUALESQUIERA GARANTÍAS DE NO INFRINGIMIENTO DE LA PROPIEDAD INTELECTUAL, CALIDAD SATISFACTORIA, ADECUACIÓN PARA UNA FINALIDAD DETERMINADA O CUALQUIER GARANTÍA SURGIDA DE CUALQUIER PROPUESTA, ESPECIFICACIÓN, MUESTRA O DE OTRA CLASE.

Esta garantía no cubre la sustitución de productos dañados por abuso, accidente, mal uso, negligencia, alteración, reparación, desastre, instalación incorrecta o pruebas incorrectas. Si el producto tuviera cualquier otro defecto, Intel se reserva la opción de reemplazar o reparar el producto sin cargo alguno, excepto los descritos a continuación, siempre que el producto se entregue con un número de autorización de devolución de material (RMA), a (a) la empresa a la que se adquirió o (b) a Intel, sólo en América del Norte (si lo adquirió en Europa, debe entregar el producto a "(a)"). Si envía el producto, debe asumir el riesgo de daños o pérdida en el transporte. Debe utilizar el embalaje original (o equivalente) y costear los gastos de envío. Intel puede reemplazar o reparar el producto con piezas o productos nuevos o refabricados, y el producto devuelto pasa a ser propiedad de Intel. Intel garantiza que el producto reparado o reemplazado no tendrá defectos materiales ni de fabricación durante el periodo que resulte mayor de los siguientes: (i) noventa (90) días desde la fecha de envío; o (ii) el periodo de tiempo restante de la garantía original de tres (3) años.

Esta garantía le otorga derechos legales concretos y puede tener otros derechos que varían según la jurisdicción. Todas las piezas o componentes que contiene este producto están cubiertos por la garantía limitada de Intel sobre este producto; el producto puede contener piezas recicladas, completamente comprobadas, garantizadas como si de piezas nuevas se tratase. Si desea obtener más información sobre la garantía, puede llamar a uno de los números indicados a continuación.

Devolución de productos defectuosos (RMA)

Antes de devolver cualquier producto, póngase en contacto con el grupo de Asistencia al cliente de Intel y obtenga un número RMA en uno de los siguientes números no gratuitos:

País	Número	Idioma
Francia	+33 (0) 1 41 91 85 29	Francés
Alemania	+49 (0) 69 9509 6099	Alemán
Italia	+39 (0) 2 696 33276	Italiano
Reino Unido	+44 (0) 870 607 2439	Inglés

Si el grupo de Asistencia al cliente comprueba que el producto es defectuoso, se podrá en contacto con el Departamento de autorización de devolución de material para que éste le envíe un número RMA que debe colocar en el envoltorio externo del producto. Intel no puede aceptar productos sin el número RMA en el paquete.

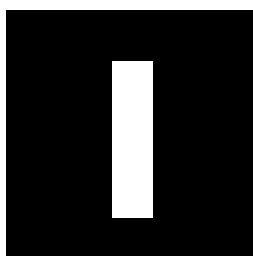
LIMITACIÓN DE RESPONSABILIDAD Y REPARACIONES

INTEL NO SERÁ RESPONSABLE DE NINGÚN DAÑO INDIRECTO O ESPECULATIVO (INCLUIDOS, SIN LIMITAR A LOS ANTERIORES, LOS DAÑOS INDIRECTOS, INCIDENTALES Y ESPECIALES) PRODUCIDO POR EL USO O POR LA IMPOSIBILIDAD DEL USO DE ESTE PRODUCTO, YA PROVENGA DE CONTRATO, NEGLIGENCIA, AGRAVIO O BAJO CUALQUIER GARANTÍA, SIN IMPORTAR QUE INTEL HAYA RECIBIDO PREVIO AVISO DE LA POSIBILIDAD DE DICHOS DAÑOS, INCLUIDOS, AUNQUE NO LIMITADOS A, PÉRDIDAS DE USO, INFRINGIMIENTO DE LA PROPIEDAD INTELECTUAL, SUSPENSIÓN DEL EJERCICIO COMERCIAL Y PÉRDIDA DE BENEFICIOS, A PESAR DE LO ANTERIOR, TODA LA RESPONSABILIDAD DE INTEL SOBRE LAS RECLAMACIONES REALIZADAS BAJO ESTE ACUERDO NO EXCEDERÁ EL PRECIO PAGADO POR EL PRODUCTO. ESTAS LIMITACIONES SOBRE LAS RESPONSABILIDADES POTENCIALES HAN CONSTITUIDO UN ELEMENTO ESENCIAL A LA HORA DE DETERMINAR EL PRECIO DEL PRODUCTO. INTEL NO ASUME NI AUTORIZA QUE NINGUNA PERSONA ASUMA EN SU LUGAR NINGUNA OTRA RESPONSABILIDAD.

Aplicaciones de control crítico: Intel deniega específicamente la responsabilidad por el uso del producto de hardware en aplicaciones de control crítico (incluidos, sólo a modo de ejemplo, los sistemas de seguridad o atención sanitaria, sistemas de control de energía nuclear o sistemas de control de tráfico aéreo o rodado) por Receptores o Subreceptores de la Licencia, y dicho uso queda enteramente a riesgo del usuario. El Receptor de la Licencia acuerda defender, indemnizar y mantener la inocencia de Intel por y contra toda reclamación surgida del uso del producto de hardware en tales aplicaciones por parte del Receptor o Subreceptor de la Licencia.

Software: El software proporcionado con el producto de hardware no está cubierto por la garantía de hardware descrita anteriormente. Si desea obtener información detallada sobre las garantías de software, consulte el acuerdo de licencia correspondiente al software incluido con el producto de hardware.

Esta garantía limitada de hardware se regirá e interpretará de acuerdo con las leyes de Inglaterra y Gales. Los tribunales de Inglaterra tendrán la exclusiva jurisdicción sobre todas las reclamaciones presentadas bajo esta garantía.



Index

A - B

- access level
 - See user accounts 79
- access level, user account 79
- accessing
 - Intel Device View 23
 - Local Management 51
- adding new users 78
- advanced settings, configure 59
- age out timer, IGMP snooping 66
- anchor port
 - in link aggregation 42, 73
- arrow keys, using 53
- asymmetric VLANs 19
- auto-partition, setting for the switch 61
- baud rate, serial port 51
- Boot PROM, version 59
- BOOTP Service, starting 56
- broadcast frames, received 103
- broadcast storm control 74
- buttons, Web Device Manager 32

C

- cable wiring 7
- cabling, guidelines 3
- collisions 102
 - viewing for individual ports 99
- community strings, changing 44
- community strings, changing (Local Management) 76
- configuration file
 - downloading 48, 80
 - See also updating 48
 - specifying path and filename 48, 80
- configure
 - 802.1p priority queues 57
 - auto-partition 61
 - community strings 76
 - Head of Line blocking 61
 - High Priority Service Ratio 61
 - link aggregation 42, 73
 - port-based VLAN 38
 - static MAC addresses 43
 - switch management options 54
 - trap receiving stations 44, 76
 - user account 35

- connecting
 - serial port 51
 - Telnet 52
- console timeout, changing 81

D

- defaults
 - communication parameters 51
 - gateway 56
 - HyperTerminal 51
 - password 52
 - username 52
- deleting user accounts 79
- Device Tree 25
 - adding a device 26
 - deleting a device 26
 - finding a device 26
 - losing contact with a device 26
 - refresh 26
- DHCP 56
- disabling
 - module ports 58
- disabling port security 68
- duplex
 - using Local Management 57, 58
 - using Web Device Manager 34

E - F

- enter key, using 53
- errors
 - collisions 102
 - CRC 101
 - dropped frames 102
 - fragments 101
 - jabber 101
 - oversize frames 101
 - total errors detected 102
 - undersize frames 102
- Ethernet Multicast Filtering
 - See also filtering 70

- filtering 69
 - Ethernet multicast 70
 - Ethernet multicast (ports) 71
 - MAC address 69
- firmware
 - displaying current version (Local Management) 59
 - See also updating 47
 - specifying path and filename (Local Management) 80
 - updating 47
- flash memory, saving changes to 54
- flow control 14
 - configuring for switch ports 34, 57
 - setting for optional module 58
- fragments 101
- frames
 - broadcast 103
 - multicast 103
 - unicast 103
 - viewing for individual ports 100

G - J

- GARP VLAN registration protocol 20
- gateway, default 56
- general information
 - viewing using Web Device Manager 46
- GVRP 96
 - configuring 41
 - See also GARP VLAN Registration Protocol 20
 - status 97
- Head of Line (HOL) blocking prevention 61
- High Priority Service Ratio 61
- hot keys, using 53
- HyperTerminal, default parameters 51
- IGMP snooping
 - on VLAN 66, 88
- IGMP, description 66
- in-band connection through Telnet 52
- ingress filtering 41

- Intel Device View 22
 - installing 22
 - starting 23
- Internet Group Multicast Protocol 20
- IP address 33
 - assigning remotely (BOOTP/DHCP) 56
 - configuring 33
 - subnet mask 56
- IP settings 33

L

- late events
 - viewing for individual ports 102
- LEDs 3
 - Matrix (stacking) module 5
 - Module A (gigabit) 5
 - port 3
 - status 3
- link aggregation 16, 42
 - anchor port 42
 - configuring with Local Management 73
 - on Web Device Manager graphic 32
- Local Management 51
 - accessing 51
 - configure management 75
 - configuring link aggregation 73
 - creating a user account 78
 - deleting user account 79
 - navigating 53
 - See also navigating 53
 - setting console timeout 81
- logging out 49
 - Web Device Manager 49

M

- MAC address
 - assigned to switch 59
 - last seen by port 100
 - See also filtering 69

- Management
 - Device Tree 27
 - See also Local Management 51
 - See also Web Device Manager 29
- Media Requirements 6
- media types, selecting the right one 6
- mirroring
 - See also ports 72
- modules 3
 - 100/1000Base-T 4
 - 100Base-LX 4
 - 100Base-SX 4
 - configuring 5
 - installing 4
 - Matrix 4
- monitoring 45
 - switch activity (with Web Device Manager) 45
- multicast frames, received 103

N - O

- navigating
 - Local Management 53
 - Web Device Manager 31
- new devices
 - installing 24
- oversize frames 101
- overstrike mode 53

P

- packet priority
 - setting for a port 34, 57
 - setting for module ports 58
- password
 - default 51
 - setting and changing 79
- Plug-in version of Intel Device View
 - installing 22
- Port
 - configuring 34

- port security 68
- port-based VLAN
 - configuring with Web Device Manager 38
 - description 17
- ports
 - adding to link aggregation 42, 73
 - adding to VLAN 39
 - enabling/disabling 34, 57
 - mirroring 72
 - setting flow control 34, 57
 - setting packet priority 34, 57
 - setting speed/duplex 34, 57
 - viewing statistics 45
 - viewing status 32
- Priority 15
- priority queues, 802.1p 57
- PVID 41

R - S

- receiving stations, sending traps to 44, 76
- RMON 28
- saving switch settings 54
- security
 - assigning MAC address 68
 - disabling for port 68
- serial port
 - baud rate 51
 - connecting through 51
 - default settings 51
- SNMP management 44
 - agent's VLAN location 56
- spacebar, using 53
- Spanning Tree 14
 - configure for ports 63
 - description 64
 - port cost 64
 - port priority 64
 - Protocol 14
 - using with VLANs 19
- speed, changing for ports 34
- Stacking 8
- subnet mask 56

- switch
 - description 12
 - serial number 59
 - viewing Boot PROM version 59
 - viewing firmware version 59

T

- tab key, using 53
- tag-based VLAN
 - adding ports 39
 - allowing IGMP snooping for 88
 - configure using Local Management 90
 - configuring with Web Device Manager 39
 - description 18
 - GVRP 41, 87
 - ingress filtering 41
 - PVID 41
 - VID 88, 89, 93, 94
- tag-based VLANs
 - description 18
- Tagged Frames 15
- Telnet, using 52
- traps
 - defining receiving stations 44, 76
 - types 76

U - V

- unicast frames, received 103
- updating 47
 - configuration file (with Web Device Manager) 48
 - firmware (with Web Device Manager) 47
- upper threshold, broadcast traffic 74
- user account
 - change access level 79

- user accounts 35
 - add users (using Local Management) 77
 - change password 79
 - create 35, 78
 - creating new account 35, 78
 - delete 36, 79
 - deleting 79
 - modifying access level 79
- user accounts, managing 78
- utilization
 - viewing for individual ports 99
- VID 18, 39, 88, 89, 93, 94
- VLANs 17
 - configuring with Local Management 82
 - configuring with Web Device Manager 37
 - port-based 17
 - tag-based
 - GVRP 41, 87
 - ingress filter 41
 - PVID 41
 - using with Spanning Tree 19
- Web version of Intel Device View
 - installing 22
 - starting 23
- Windows version of Intel Device View
 - installing 22
 - starting 23

W

- Web Device Manager 30
 - accessing 30
 - buttons 32
 - community strings 44
 - configuring IP settings 33
 - configuring link aggregation 42
 - configuring trap receivers 44
 - configuring user accounts 35
 - navigating 31
 - port status 32
 - setting port flow control 34
 - setting port speed/duplex 34
 - setting priority queues 34
 - updating configuration files 48
 - using screens 32
 - viewing and configuring switch
 - information 46

Intel Customer Support

You can purchase a range of support services including hardware, software, phone, and on-site installation services. Services are designed and packaged for ease of ordering and provide reliable, flexible support for your networking equipment. For details about Intel® NetStructure™ Support Services, go to www.intel.com/network/services.

Worldwide Access to Technical Support

Intel has technical support centers worldwide. Technicians who speak the local languages staff many of the centers. Visit our Web site at support.intel.com or contact your local dealer/distributor.

United States and Canada only

For support, call **(800) 838-7136** or **(916) 377-7000**.

Japan only

For support, call **+81-298-47-0800**.

Other areas

(Access number + 800-838-7136)

For support in other countries, use the following table to dial the toll-free support number. Using the table, locate the country from which you are calling, dial the access number, wait for the dial tone, and then dial 800-838-7136.

Country	Access Number
Australia	1-800-881-011
Austria ^{1 4}	022-903-011
Belgium ¹	0-800-100-10
China ³	10811
Denmark	8001-0010
Finland ¹	9800-100-10
France (Includes Andorra)	19-0011
Germany	0130-0010
Hong Kong	800-1111
India ⁵	000-117

Country	Access Number
Indonesia ²	001-801-10
Italy (Includes Vatican City) ¹	172-1011
Korea ¹	0-911
Malaysia ⁴	800-0011
Netherlands ¹	06-022-9111
New Zealand	000-911
Norway	800-190-11
Pakistan	0080001001
Philippines	105-11
Poland ^{1 3}	0-0-800-111-1111
Portugal ³	05017-1-288
RSA (South Africa)	0-800-99-0123
Russia ^{1 2 3}	755-5042
Singapore	800-0111-111
Spain	900-99-00-11
Sri Lanka	430-430
Sweden	020-795-611
Switzerland ¹	0-800-550011
Taiwan ¹	0080-10288-0
Thailand ⁵	0019-991-1111
United Kingdom (BT) ³	0800-89-0011
United Kingdom (Mercury) ³	0500-89-0011
Vietnam	12010288

Notes

- ¹ Public phones require coin deposit
- ² Use phones allowing international access
- ³ May not be available from every phone
- ⁴ Public phones require local phone payment through the call duration
- ⁵ Not available from public phones

